WDS1U2PGE EPON OLT Equipment

User Manual - EMS Software Part

Version : V1.1

©Statement

Copyright ©2012. All Rights Reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without the prior written consent.

The information in this document may be update at any time due to product versions upgrade or any other reasons. Unless otherwise agreed, this manual is for reference only. All statements, information and recommendations in this manual do not constitute the warranty of any kind, express or implied.

Please contact your suppliers to get the latest version of this document.

About This Manual

This document is one of the WDS1U2PGE OLT equipment user manuals. The contents of this document include EMS software installation and operation guidelines. Users should learn this document first when beginning to operate FD1002S OLT device.

The related documents for WDS1U2PGE OLT device are:
《WDS1U2PGE OLT - Device Installation User Manual》
《WDS1U2PGE OLT- CLI Operation User Manual》

Revision History

VER	DATE	
1.0.01	2013.10.9	
1.1	2015.4.1	

Table of Contents

©STATEMENT 2

ABOUT THIS MANUAL 2

REVISION HISTORY 2

1 1 SOFTWARE INTRODUCTION 5

1.1 BRIEF VIEWS 5

1.2 FUNCTIONAL FEATURES 5

2 EMS SOFTWARE INSTALLATION 5

2.1 DATABASE INSTALLATION 5

2.2 EMS SOFTWARE INSTALLATION 11

3 EMS STARTUP 12

3.1 MYSQL DATABASE STARTUP 12

3.2 EMS SOFTWARE STARTUP 12

4 EMS SOFTWARE FRAME INTRODUCTION 14

4.1 4.1 MAIN FRAME OVERVIEW 14

4.2 DEVICE MANAGEMENT WINDOW 16

5 MANAGEMENT OBJECT ADD/DELETE 17

5.1 LOCATION ADD/DELETE 17

5.2 ADD/DELETE DEVICE 18

6 FD1002S OLT MANAGEMENT 20

6.1 OLT CHASSIS MANAGEMENT 20

6.2 SWITCH AND CONTROL CARD MANAGEMENT 21

6.2.1 Device Basic Information and System Configuration 21

6.2.2 In-band Network Interface Management 22

6.2.3 User Management 23

6.2.4 Trunk Management 23

6.2.5 Configuring VLAN 24

6.2.6 Port Mirroring 26

6.2.7 Switch Port Management 27

6.2.7.1 Port Property Settings 27

6.2.7.2 Port Status 28

6.2.8 ONU Authentication 29

6.3 PON CARD MANAGEMENT 31

6.3.1 Basic Information View 31

6.3.2 Basic Operation 31

6.3.3 OLT Management 31

6.3.4 OLT Bridge Configuration 32
6.3.5 ONU P2P 33
6.3.6 LLID 33
6.3.6.1 Configuring LLID 33
6.3.6.2 Configuring Logic Link SLA 34
7 ONU MANAGEMENT 35
7.1 ONU MANAGEMENT INTRODUCTION 35
7.2 ONU BASIC INFORMATION 37
7.2.1 LED Indicator 37
7.2.2 Basic Information 37
7.2.3 Basic Operation 38
7.3 RSTP CONFIGURE AND PORT ISOLATION 38
7.4 ONU PORT MANAGEMENT 39
7.4.1 Port Working Status 39
7.4.2 Port Bridge Mode 40
7.4.3 MAC Address Management 41
7.4.4 Ingress Policy and Egress Shaping 41
7.5 ONU LOOPBACK TEST 42
7.6 ONU IGMP SNOOPING 43
7.7 ONU ACL CONFIGURATION 45
7.8 ONU VLAN CONFIGURATION 47
7.9 ONU LOGICAL LINK MANAGEMENT 52
7.9.1 Logical Link Status Management 52
7.9.2 Logical Link MAC Address Management 53
7.9.3 Logical Link SLA Management 54
8 ALARM MANAGEMENT 54
8.1 ALARM RULE CONFIGURATION 55
8.2 ALARM QUERY 55
9 OPERATION LOG MANAGEMENT 57
10 DATABASE MAINTENANCE 57
11 USER ACCOUNTS MANAGEMENT 58
12 SYSTEM UPGRADE 59
END 62

1 1 Software Introduction

1.1 Brief Views

EMS (Element Management System) software is a C/S architecture integrated device management platform, which is designed based on SNMP protocol. Now, it is mainly used for managing EPON series products.

EMS need following runtime environment：

- OS：Windows2000、Windows XP、Windows NT、Windows 7、Windows8
- Hardware：CPU 2.4GHz , 512M memory
- Software：JAVA 1.5, MySql 5.0

1.2 Functional Features

EMS software has following main features:

- Based on standard SNMP protocol
- Support multiple client access, C/S architecture
- Support integrated management all our EPON series products
- Support auto topology or modify manually, and multi-layer map view
- Support configuration operation on all EPON products functions
- Support multiple level operation authority
- Real-time and history alarm record view, search and save
- Operation history record trace and save
- Use independent database and support data backup and import
- Support performance monitor and traffic counters statistic
- Support third-party database platform

2 EMS Software Installation

EMS software installation needs two steps, database installation and EMS software setup. And database need to be installed before software setup.

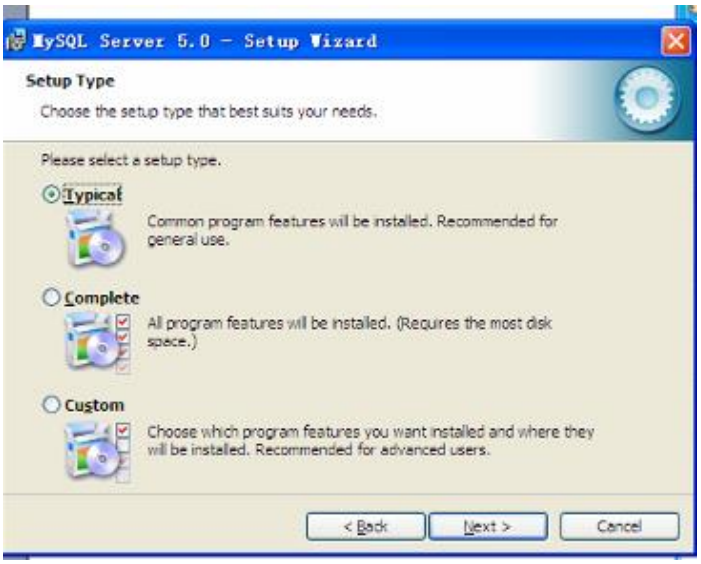
2.1 Database Installation

The opened third part database software Mysql is used by EMS. The Mysql setup programs provided in CD which is shipped with products can be directly used or you can download it from internet. Remember 5.0 or higher version is compatible with EMS software.

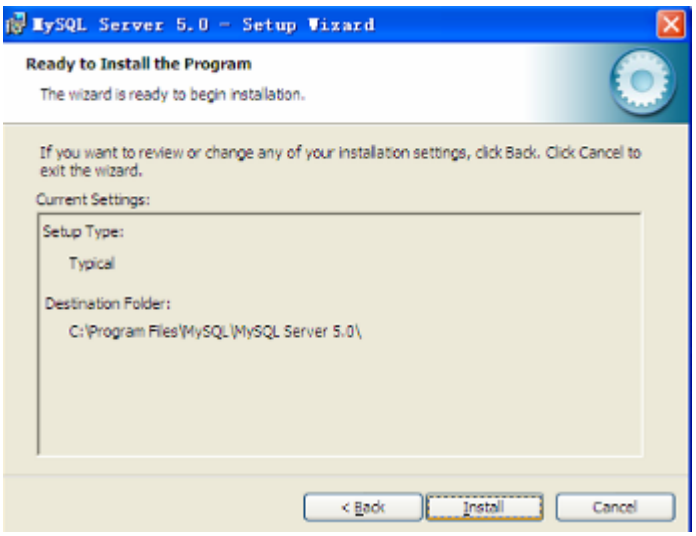
According to following steps to install Mysql database:

MySQL Server 5.0 - Setup Wizard
Welcome to the Setup Wizard for MySQL Server 5.0
The Setup Wizard will install MySQL Server 5.0 release 5.0.24a on your computer. To continue, click Next.
WARNING: This program is protected by copyright law.
MySQL
< Back
Next >
Cancel

Click **Next** to continue:


MySQL Server 5.0 - Setup Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Typical
Common program features will be installed. Recommended for general use.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
< Back
Next >
Cancel

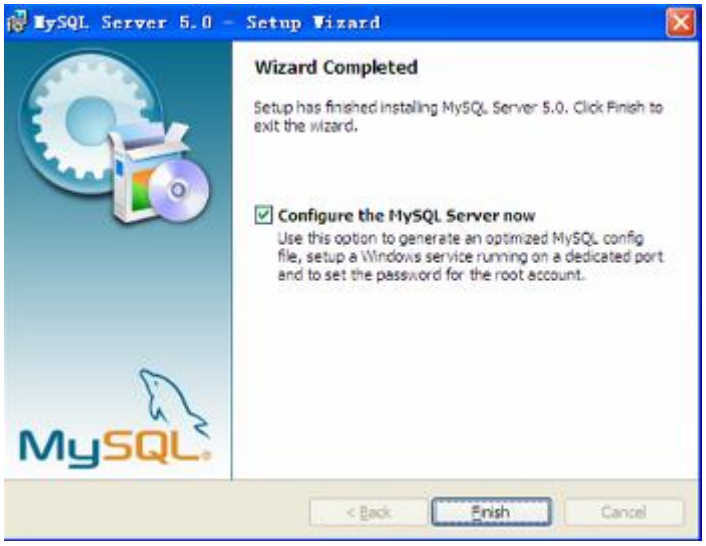
Choose **Typical** setup type.


MySQL Server 5.0 - Setup Wizard
Ready to Install the Program
The wizard is ready to begin installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Current Settings:
Setup Type:
Typical
Destination Folder:
C:\Program Files\MySQL\MySQL Server 5.0\
< Back
Install
Cancel

Click **Install** to begin setting up.

MySQL.com Sign Up - Setup Wizard
MySQL.com Sign-Up
Login or create a new MySQL.com account.
Please log in or select the option to create a new account.
Create a new free MySQL.com account
If you do not yet have a MySQL.com account, select this option and complete the following three steps.
Login to MySQL.com
Select this option if you already have a MySQL.com account. Please specify your login information below.
Email address:
Password:
Skip Sign-Up
Next >
Cancel

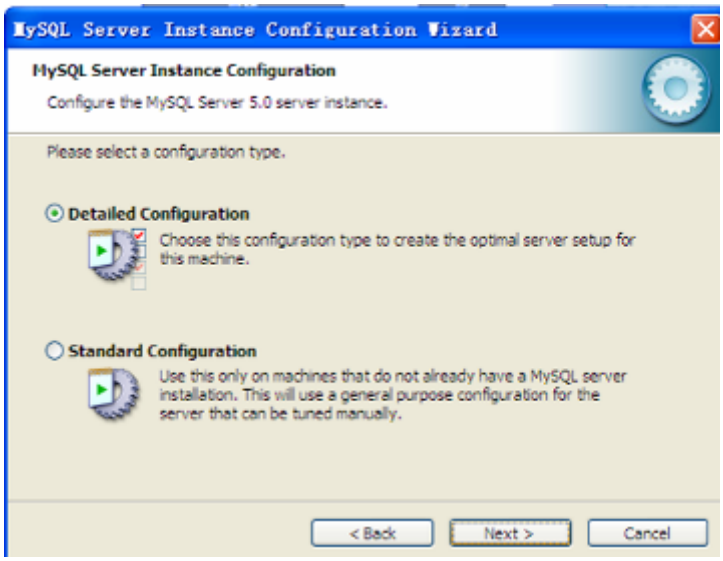
Choose **Skip Sign-Up**, go to next step.


MySQL Server 5.0 - Setup Wizard
Wizard Completed
Setup has finished installing MySQL Server 5.0. Click Finish to exit the wizard.
Configure the MySQL Server now
Use this option to generate an optimized MySQL config file, setup a Windows service running on a dedicated port and to set the password for the root account.
MySQL
< Back
Finish
Cancel

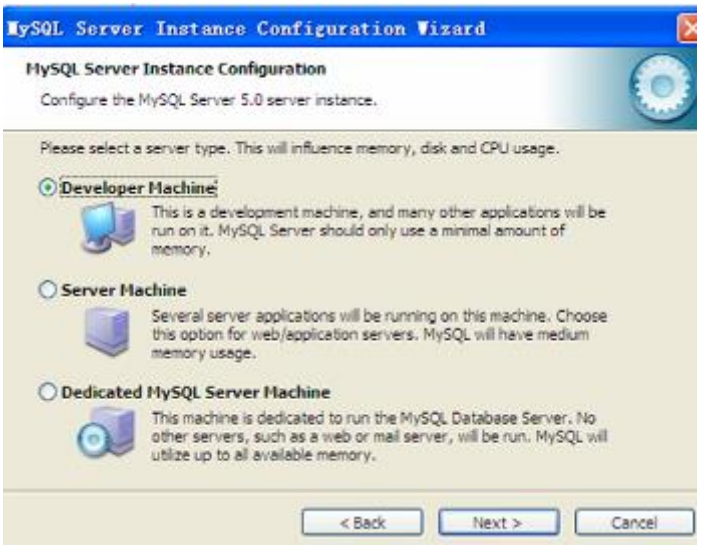
Installation finished, choose “Configure the MySQL Server now” option to begin database software configurations:

MySQL Server Instance Configuration Wizard
Welcome to the MySQL Server Instance Configuration Wizard 1.0.8
The Configuration Wizard will allow you to configure the MySQL Server 5.0 server instance. To Continue, click Next.
MySQL
Next >
Cancel

Database configuration wizard startup, click **Next** to continue:


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select a configuration type.
Detailed Configuration
Choose this configuration type to create the optimal server setup for this machine.
Standard Configuration
Use this only on machines that do not already have a MySQL server installation. This will use a general purpose configuration for the server that can be tuned manually.
< Back
Next >
Cancel

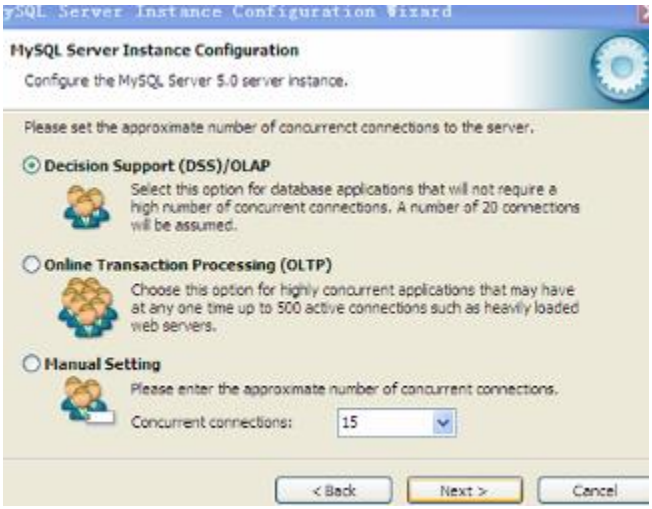
Choose “Detailed Configuration” (default option) to go to next step:


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select a server type. This will influence memory, disk and CPU usage.
Developer Machine
This is a development machine, and many other applications will be run on it. MySQL Server should only use a minimal amount of memory.
Server Machine
Several server applications will be running on this machine. Choose this option for web/application servers. MySQL will have medium memory usage.
Dedicated MySQL Server Machine
This machine is dedicated to run the MySQL Database Server. No other servers, such as a web or mail server, will be run. MySQL will utilize up to all available memory.
< Back
Next >
Cancel

Choose “Developer Machine” (default option), click **Next**:

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select the database usage.
Multifunctional Database
General purpose databases. This will optimize the server for the use of the fast transactional InnoDB storage engine and the high speed MyISAM storage engine.
Transactional Database Only
Optimized for application servers and transactional web applications. This will make InnoDB the main storage engine. Note that the MyISAM engine can still be used.
Non-Transactional Database Only
Suited for simple web applications, monitoring or logging applications as well as analysis programs. Only the non-transactional MyISAM storage engine will be activated.
< Back
Next >
Cancel

Choose “Multifunctional Database”（default option） to continue:


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the approximate number of concurrent connections to the server.
Decision Support (DSS)/OLAP
Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed.
Online Transaction Processing (OLTP)
Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers.
Manual Setting
Please enter the approximate number of concurrent connections.
Concurrent connections:
15
< Back
Next >
Cancel

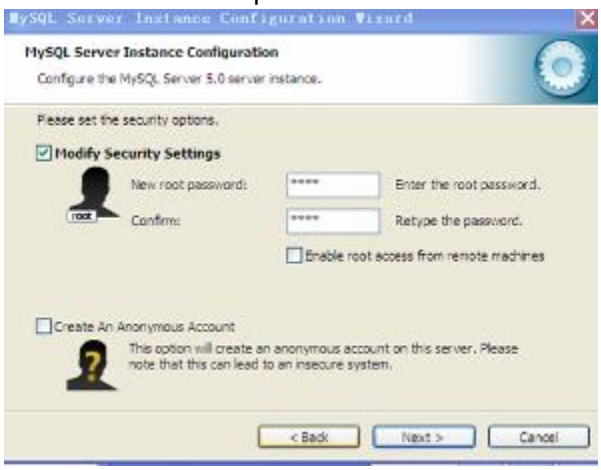
Choose “Decision Support(DSS)/OLAP”（default option）, click **Next**:

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select the default character set.
Standard Character Set
Hello!
Makes Latin1 the default charset. This character set is suited for English and other West European languages.
Best Support For Multilingualism
Make UTF8 the default character set. This is the recommended character set for storing text in many different languages.
Manual Selected Default Character Set / Collation
Please specify the character set to use.
Character Set:
utf8
< Back
Next >
Cancel

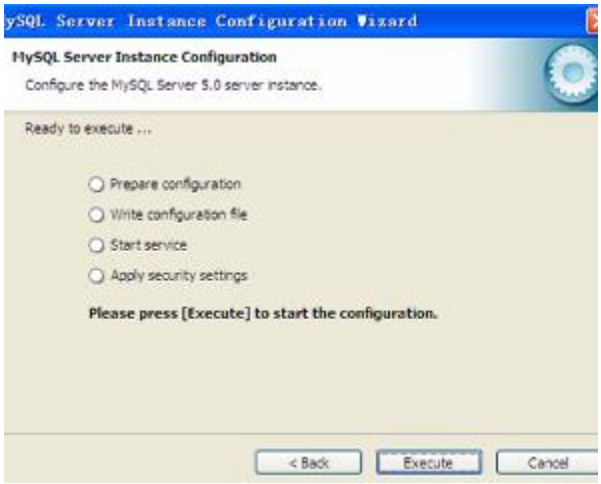
Choose “Manual Selected Default Character Set/Collation” option, and specify “Character Set” as “**utf8**” type to go to next step:

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the Windows options.
Install As Windows Service
This is the recommended way to run the MySQL server on Windows.
Service Name:
MySQL
Launch the MySQL Server automatically
Include Bin Directory in Windows PATH
Check this option to include the directory containing the server / client executables in the Windows PATH variable so they can be called from the command line.
< Back
Next >
Cancel

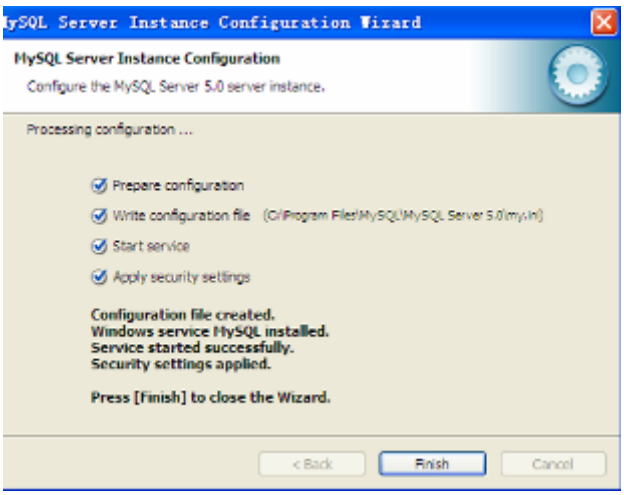
Choose “Install As Windows Service” option（default option） and“Include Bin Directory in Windows PATH” option（Note: this is not default option）, click **Next**:


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the security options.
Modify Security Settings
New root password:
Enter the root password.
Confirm:
Retype the password.
Enable root access from remote machines
Create An Anonymous Account
This option will create an anonymous account on this server. Please note that this can lead to an insecure system.
< Back
Next >
Cancel

Choose “Modify Security Settings” option, and set “New root password” as “**1234**”, and set it again in “Confirm” text field to confirm this security password. This password is used by EMS software to access MySQL database and must be set correctly. Then click **Next** to continue:



Come here, MySQL database configuration wizard finished, click **Execute** to startup.



As above interface, showing MySQL database installation, configuration and startup successfully finished, click **Finish** to complete all the installation steps.

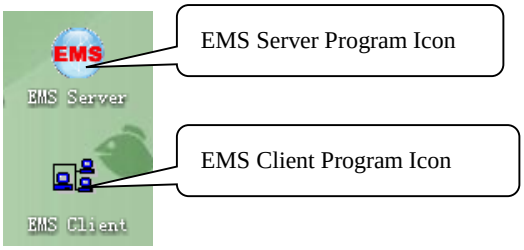
2.2 EMS Software Installation

EMS software can be installed when MySQL database has been successfully installed. Run EMS set up program directly, and then following the installation wizard to finish all the installation steps. There are no special configuration options during the whole installation process.

The initial startup interface is as following:

EMS - InstallShield Wizard
Preparing to Install...
EMS Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Decompressing: EMS.msi
Cancel

After EMS has been successfully installed, there will be two program icons created on the desktop and the installation directory. Typically as following appearance:



EMS software installed finished.

Note: EMS can be directly startup when set-up finished, PC restart is not needed.

3 EMS Startup

3.1 MySQL Database Startup

MySQL database must be startup before EMS software. Normally, MySQL should has been running up when configuration wizard successfully finished. Following method can be used to verify if MySQL database is already running up.

Right click My Computer icon, select “manage” option and then open the “service” window to verify if the “MySQL” service status is “started”.

3.2 EMS Software Startup

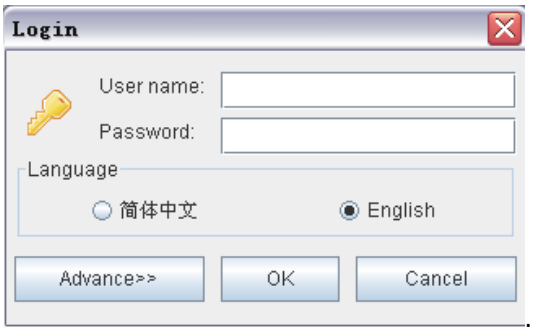
EMS software is C/S structure, including **Server** and **Client** two parts. **Server** program must be started first, and **Client** program should be run up when **Server** has been successfully started.

Double click **EMS Server** program icon to run it. There will be a **Server** icon located on the program running field, typically as following:

Note: EMS Server will take several seconds, normally it will not longer than 30 seconds. If the program running icon can’t be found there, EMS Server startup failed. In this condition, you should check to verify if the installation requirements are satisfied and if the MySQL database is successfully configured and started.

After EMS Server has been started, EMS Client program can be run up. Client and Server program can run on a same computer or a different computer, just need the network between them communication well.

Following logging window will appear after the Client software successfully started.



If Server and Client software are installed on a same computer, you should just input the correct username and password. If they run on different computer, you need set the Server's IP Address through the **Advance** configuration part. The typical interface is as following.

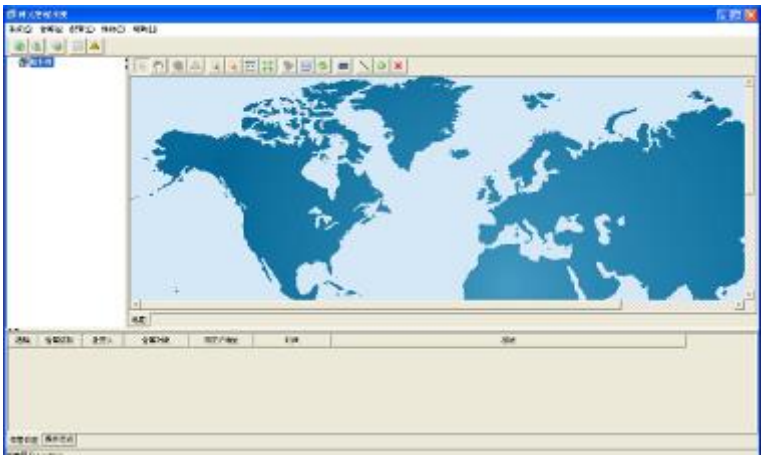
As above, **Poll Server** field is the IP Address (e.g.: "192.168.10.3") of the computer on which EMS Server is running. The other fields, **Port** and **Timeout** use the default value normally. If the transmission delay between **Server** and **Client** computers is not so good, you can change the default Timeout value to a larger one.

Note:

*1) The default **Poll Server** IP Address value is "127.0.01", which is the Loopback Address of the local computer. You need not change this value to other Address if the Client software runs on the same computer with Server software.*

*2) The default username and password are "**admin**" and "**1234**". You can change them when logging in.*

The main software interface will appear when successfully log in. The typically initial window is as following:

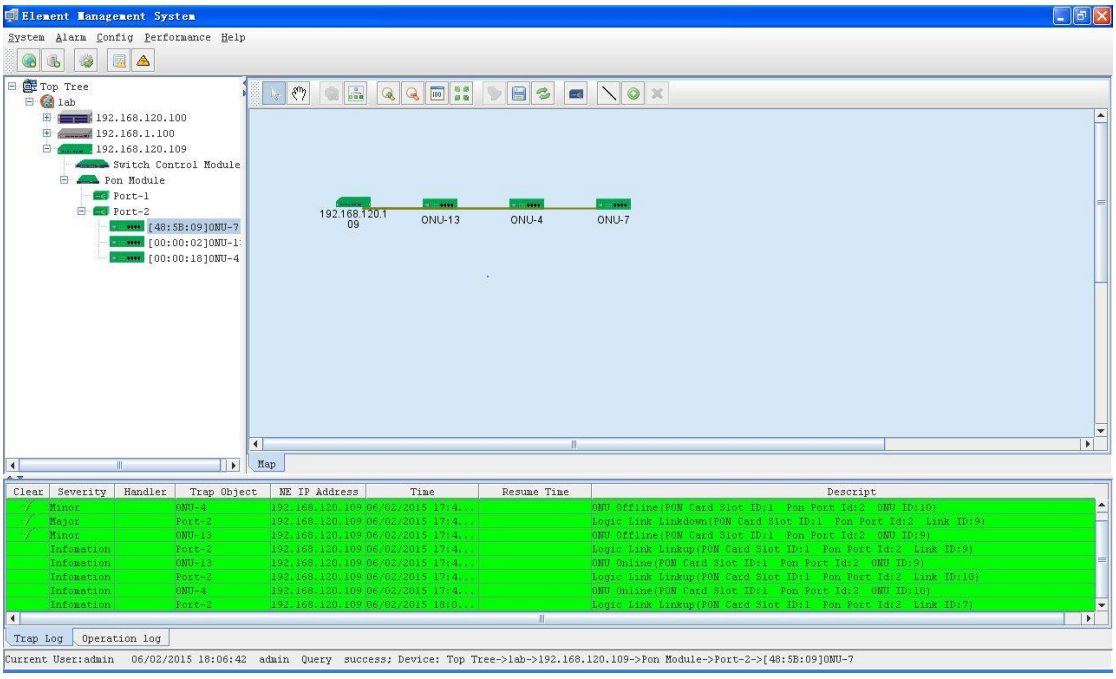


By now, EMS Server and Client software has been successfully start up

4 EMS Software Frame Introduction

4.1 4.1 Main Frame Overview

After successfully login, software comes to main frame. Following is a typical appearance.



As above figure, main frame contain following several parts:

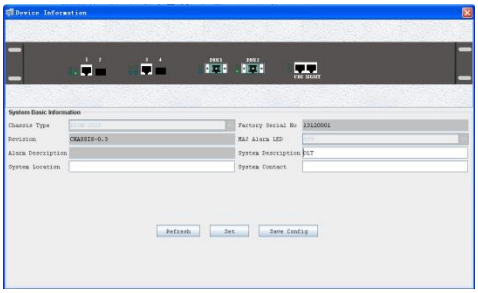
	ELEMENT	FUNCTION
1	Main Menu	Main menu contain **System**, **Alarm**, **Configure**, **Performance** and **Help** parts. Their main features are as

		follow: ➢ System Menu Including **System Configuration**, **MIB Browser**, **Database Maintenance** and **User Manage**, etc. ➢ Alarm Menu **Alarm Query**, **Configure Trap Rule** and **System Log** are within this menu. ➢ Configuration Menu **Top-tree update**, **device add/delete**, **device configuration**, **map update** and **device upgrade** features are located in this menu. ➢ Performance Menu Including performance monitor and alarm threshold configuration. ➢ Help Menu Change software skin, language and **About** information.
2	Top-tree Device List	The Top-tree list contains all the added and accessed devices managed by EMS. Through this device list, manager can view some visual device information, such as online or not, alarm status and location info etc. Double click the device icons can navigate to their management interface window. FD1002S OLT has 5 type management objects, including chassis, switch and control card, PON card, PON port and ONU device.
3	Topology Shortcut Bar	Use these buttons to manage device icons on the background map.
4	Topology Map Window	Topology Map window is the main area of EMS. The topology map of managed device is displayed here. For convenience of managing, manager can move device icons to their installation locations which are normally matched with the background map. By double click the device icons located on the map, manager can open the corresponding device management window to operate. In this area, manager can also redraw, add or delete the passive network components manually, such as fiber link

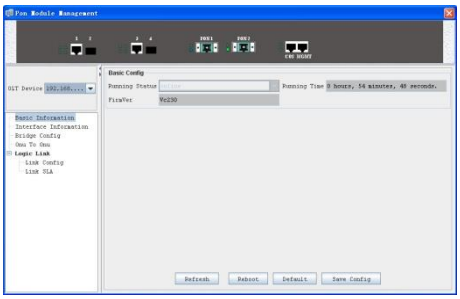
		and splitter device, in order to make them meet with the actual network deployment.
5	Alarm and Log Window	This window located on the bottom of the main frame, including **Alarm Log** and **Operation Log** page. Alarm log page shows and records the real time alarm information, including alarm object, occur time and alarm content. Operation log page shows and records the manager's operation records, in order to trace back when needed.

4.2 Device Management Window

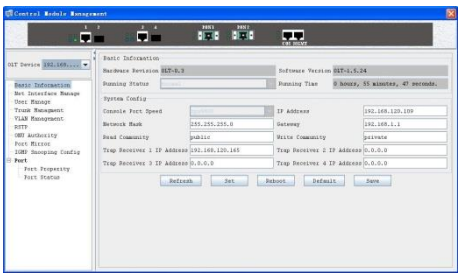
For device management, EMS is mainly through the corresponding device management window to operate. Through the **Configuration** menu or double click the device icons located on Top-tree or topology map, manager can open the device management windows. Following are several typical examples:



Device Basic Information Windows



PON Card Windows



Switch and Control Card Window

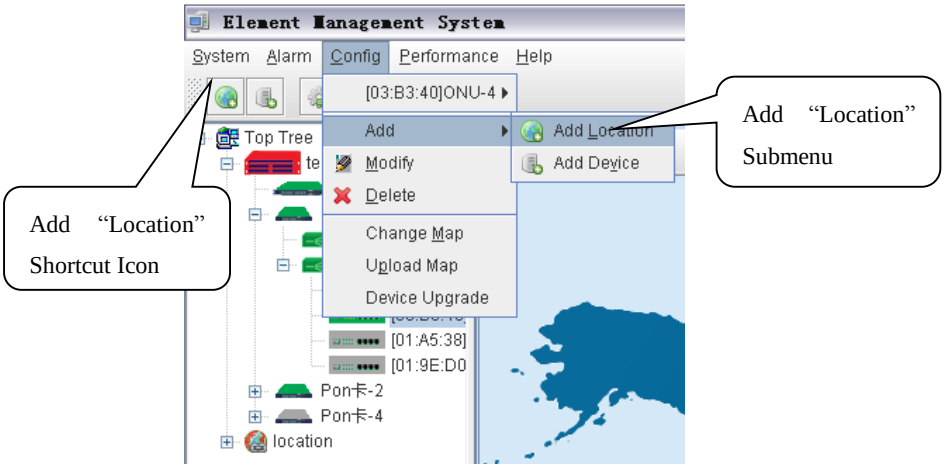
ONU Management windows

5 Management Object Add/Delete

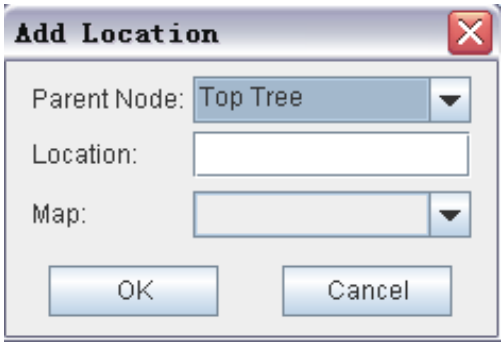
5.1 Location Add/Delete

For convenience of managing numerous devices, divide them in different regions according to their deployed locations is normally needed. According to following steps to divide management regions:

1) Add a **Location** node on the Top-tree list. Showing as follow:



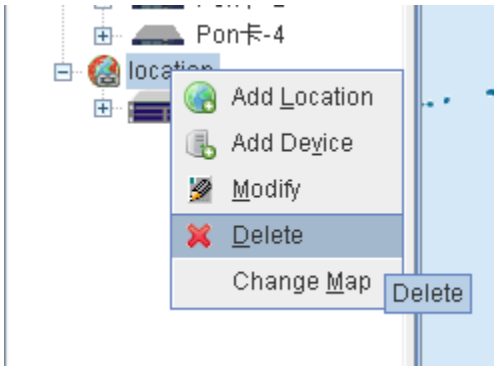
As above figure, through **Add Location** menu or its shortcut, open add location operate window, as following:



Operation steps:

i. Select the parent node for new added node;
ii. Input the name of new node;
iii. Select map for the new location node (The map should be upload first), when select this node on top-tree, the topology area will apply this map;

2) Location node delete

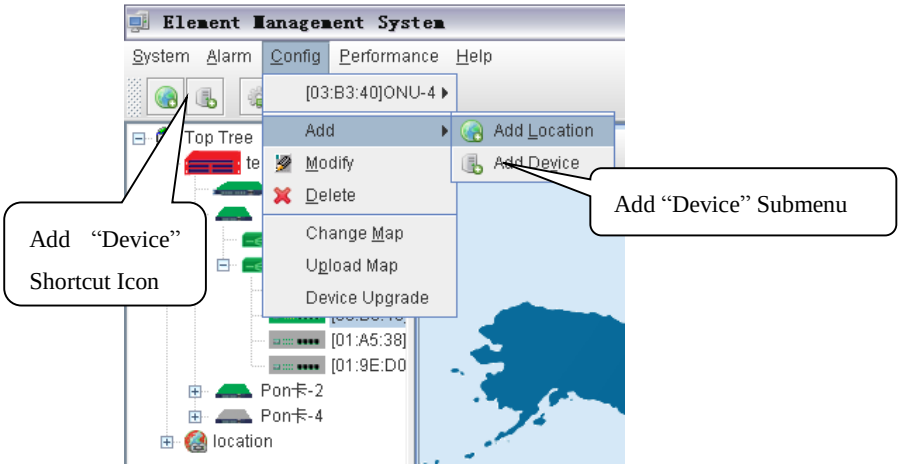


As above figure, right click the selected location node and delete it.

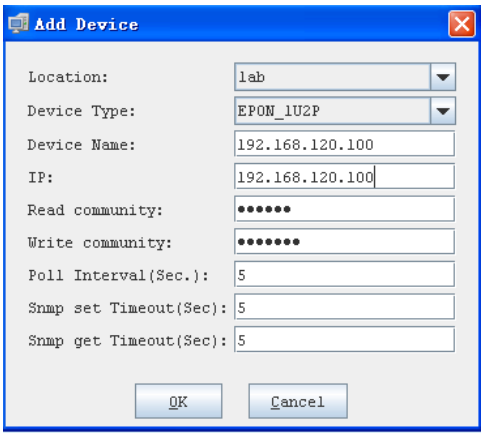
5.2 Add/Delete Device

The managed element device should be added to EMS manually. According to following steps to add a WDS1U2PGE OLT device to EMS。

1) WDS1U2PGE device add



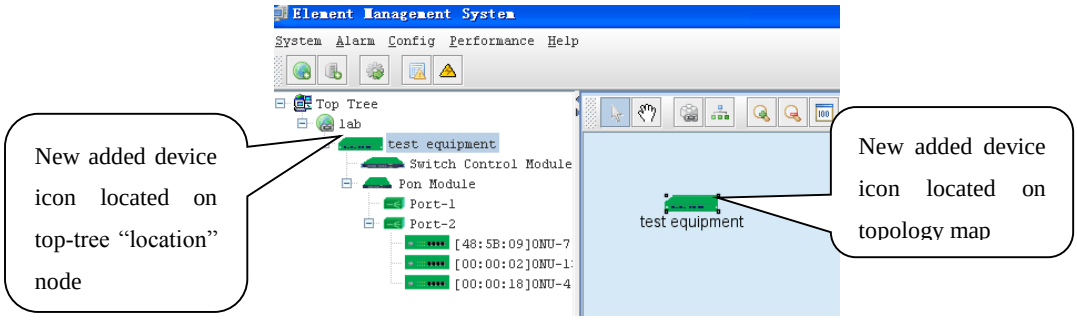
As above figure, through **Add Device** sub-menu or its shortcut to open the device add window.



As above figure, the new added device need configure following parameters:

- ✓ Location
  Select the location node where the added device should be located.
- ✓ Device Type
  Select the device type for the new added device. EMS can manage WDS1U2PGE OLT and other EPON products. So, it is needed to select correct device type. Select **EPON_1U** type for WDS1U2PGE OLT equipment.
- ✓ Device Alias
  In order to recognize the managed device easily, a suitable alias is normally needed instead of IP Address or MAC Address. This device alias will be displayed on top-tree list.
- ✓ IP Address
  Input the management IP Address of the new added element device, which can be in-band or out-band IP Address.
- ✓ Read and Write Community
  EMS software is designed based on SNMP protocol to communicate with managed devices. Read and write community is used by SNMP protocol as access password. Community value input here should be the same with which configured in managed device, such EMS can communicate with the managed device successfully.
- ✓ Polling Interval and SNMP Read and Write Timeout Value
  EMS software will poll the managed device periodically with a configured time interval. Normally, the poll interval can use the default value. SNMP read and write timeout values are the longest wait time for EMS to wait response from managed device. Usually, the default value is suitable. Manager can also revise these values according to the real network performance situation.

When the above parameters are configured, click **OK** button to finish the device add operation. When success, the new added device's icon will appear on top-tree list and topology area. Showing as following figure:



Note: For FD1002S OLT device, only the chassis node need to be added manually, other part such as equipped card and accessed ONU device need not to be added.

These devices will be detected automatically.

2) Delete WDS1U2PGE device

Obsolete or unwanted device on top-tree list can be deleted from EMS. Right click on the selected device icon and select Delete option to delete a device.

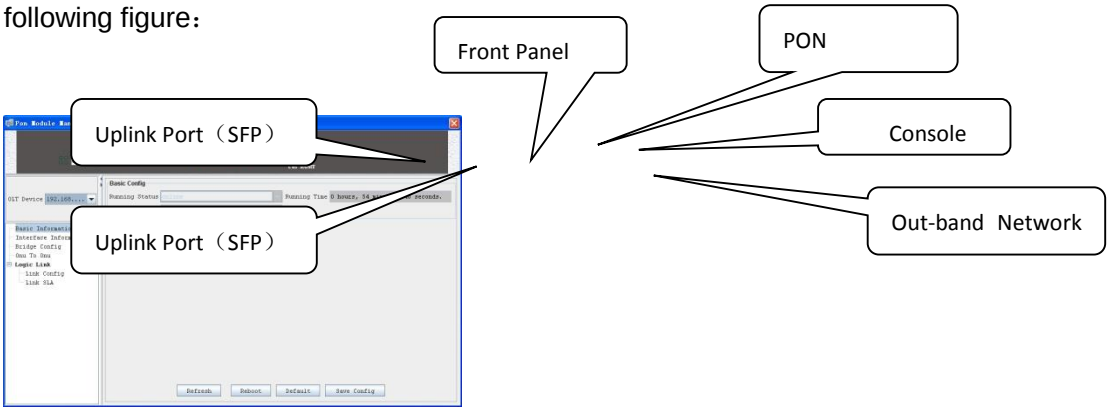
Note：

i. *Deleted device can't be restored and need to be added when need.*
ii. *All the information of the deleted device will also be removed from EMS.*
iii. *None any configurations on the deleted device itself will be changed。*

6 FD1002S OLT Management

6.1 OLT Chassis Management

Double click the OLT chassis icon to open the chassis management window. Typically as following figure：



OLT chassis management includes following several parts.

Front Panel

Four uplink ports, two PON port, one console port, one out band network management port.. Led Indicator located on the card panel graphic display the card's real time working status.

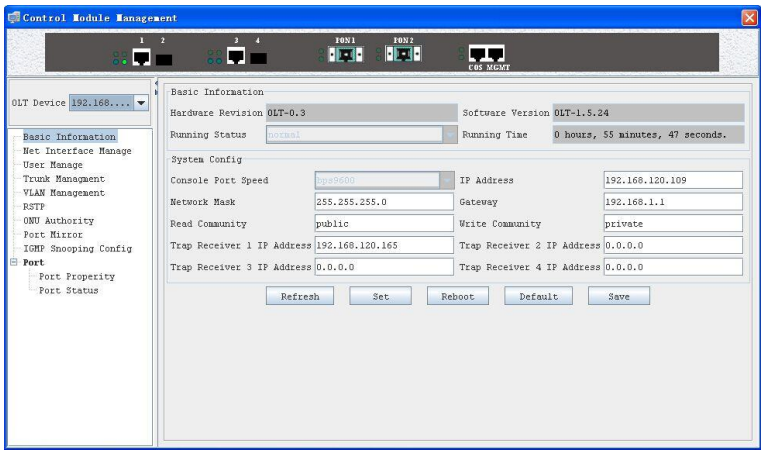
When EMS can't connect with the OLT the windows will change to gray color.

Basic Information

The basic information of device type , SN, Version, Alarm Status, System Description, Installation location and manager contact information.

6.2 Switch and Control Card Management

Double click switch and control card icon on top-tree list or the card panel icon located on chassis management window to open the switch and control management window.
Typical as following figure:：



Following management features are contained on this window:：

- Get or set device configuration information, such as IP Address, Trap Receiver Address, SNMP parameters, etc；
- Get or set management user information;
- TRUNK management of switch part;
- QINQ management of switch part;
- VLAN management of switch ports
- RSTP management of switch part;
- Port Mirror management of switch part;
- Status and configuration of switch ports;
- ONU Authority management;
- Display status, attribute of port

Following sections in this part introduce the management features contained on the switch and control card management window.

6.2.1 Device Basic Information and System Configuration

Open **Basic Information** windows.

Basic Information

Include device type, serial No, software and hardware version, running status and time information.

System Configure

Configure or check the IP Address, Subnet Mask and Default Gateway.

Note：

1) The network parameters configured here are for the out-band interface of WDS1U2PGE OLT device.
2) Out-band IP and in-band IP can't on the same network segment.
3) Usually, EMS will lost the connection with managed device when change the network parameters. Manager should change the network parameters of the managed object in EMS to the same value with the parameters configured in the device itself to recover the connection.

Configure or Check SNMP Read/Write Community

Note:

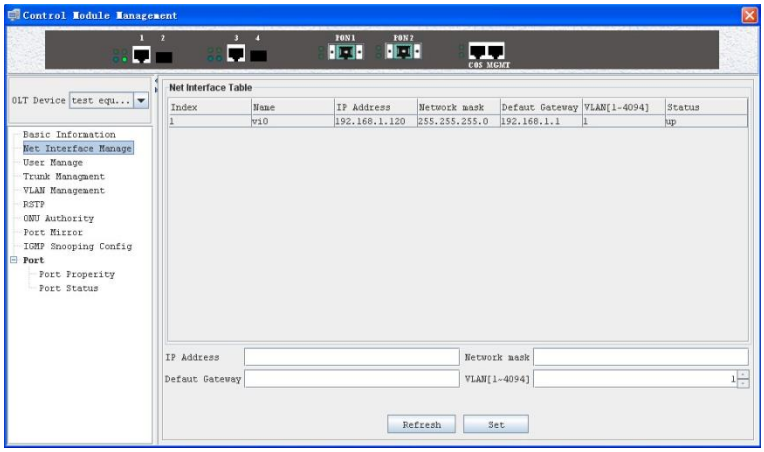
1) The Community values configured here are the parameters of the managed device itself.
2) EMS should use the same Community values to access the managed device.

Configure or Check TRAP Receiver Address

The TRAP receiver address is the destination IP Address where device alarm information is sent. When there are alarm occurred, these alarm information will be sent to these configured target IP Address. Usually, the TRAP receivers are those computer servers on which EMS software is installed. Four receiver IP Address can be configured at most.

6.2.2 In-band Network Interface Management

Open "**Network Interface Management**" page, typically as following figure：



FD1002S supports In-band and Out-band two network management interfaces. Any one of the eight uplink port can be used as In-band management port without any special specified.

Now, one network interface identified as “vi0” can be used as in-band network interface. Manager can configure its network parameters on this page, such as IP Address, Subnet Mask, Default Gateway and Management VLAN. This network interface can also be disabled.

Note：

1) The default configuration is: enabled, IP Address:192.168.1.100,Management VLAN: disable (VLAN 1);
2) In-band network IP Address can’t be configured as the same network segment with the Out-band IP Address;

6.2.3 User Management

Open “**User Manage**” page.

This page contains users’ information which is used to access the CLI management interface.

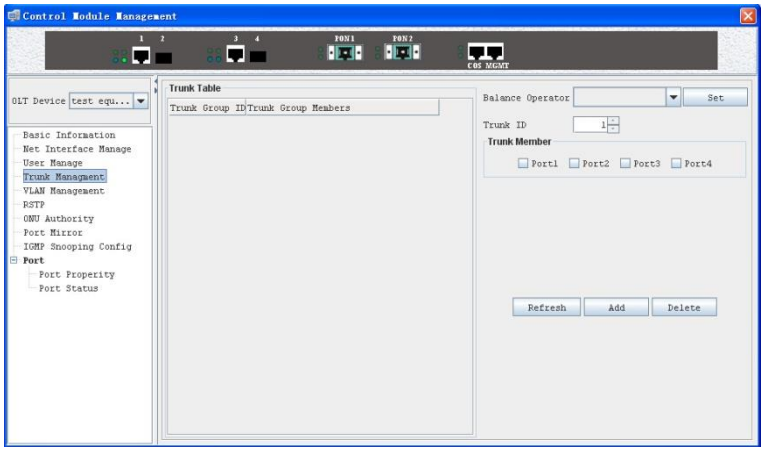
Note:

1) *The users list in this page is used to access CLI interface and not used to login EMS software.*
2) *Now, the CLI users information cannot be modified in EMS, it can be done through CLI interface.*

6.2.4 Trunk Management

WDS1U2PGE supports IEEE802.3ad Link Aggregation standard trunk protocol. Trunk allows very high bandwidth interfaces to be created by bundling multiple physical links into a single logical link. Traffic forwarded to the trunk interface is load-balanced across the physical links, thus achieving an effective bandwidth close to the aggregate bandwidth of each of the port members of the trunk group.

Open “**Trunk Management**” page. Following figure shows a Trunk configuration example.：



WDS1U2PGE TRUNK features：

- ✓ TRUNK can applied on all four uplink ports;
- ✓ Support t trunk group at most；
- ✓ Each TRUNK group support two physical ports(Only support port1 and port3 configured to one group, port2 and port4 TRUNK configured to one group)；

EMS Trunk management features supported in EMS are as following:

Trunk Table

This table displays all the configured Trunk groups and their port members. Trunk ID is used to identify one Trunk group uniquely.

Trunk Group Add

Allocate an unused Trunk ID, choose the port members for this group (only those un-allocated ports can be chosen), then click **Add** button to create a new Trunk group. The new added group and its members will be displayed in “**Trunk Table**”.

Trunk Group Delete

Select a Trunk group entry to be deleted in “**Trunk Table**” and click **Delete** button to delete it. Click “Refresh” can get the running information of TRUNK.

6.2.5 Configuring VLAN

VLAN (Virtual Local Area Network) is the standard mechanism used today to partition a single Layer 2 bridging domain into multiple, separate, independent bridging domains. Conceptually, each VLAN constitutes a bridged network.

VLANs provide many useful features such as:

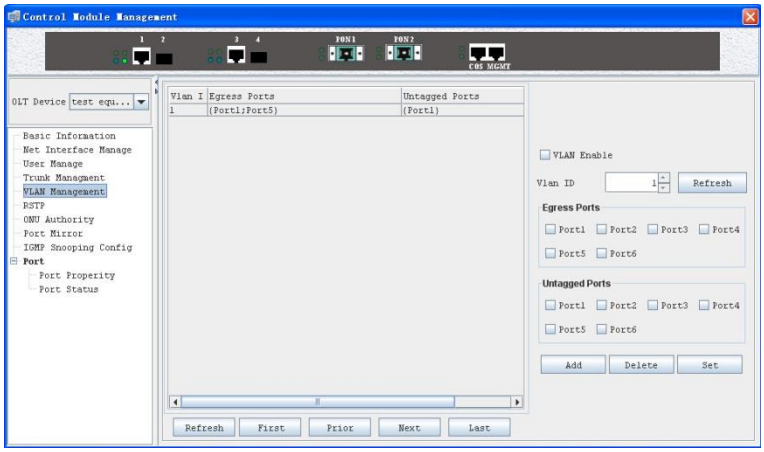
- Better utilization of bandwidth by reducing flooding of Broadcasts, Multicasts, and unknown Unicast packets to relevant ports only.

- Natural mechanism to separate traffic with different protocols or departmental traffic.
- Increased security by preventing access between VLANs. For example, networks with sensitive information such as marketing and finance can be separated from the rest of the network.

FD1002S OLT equipment switch engine is fully compliant with the IEEE802.1Q VLAN standard and has following main features.

- ✓ Support Port-based VLAN and IEEE802.1Q VLAN;
- ✓ Support full 4K VLAN group, VID range 1~4095;
- ✓ All switch ports, including uplink ports and downlink ports support VLAN partition;
- ✓ VLAN 1 is the system reserved VLAN, it includes all switch ports, all ports is UNTAG mode;

Open "**VLAN Management**" page, typically as following:



VLAN Enable/Disable:

Use the **VLAN Enable** option, manager can enable or disable VLAN feature. When disabled, all ports working on VLAN Unaware mode.

Add a new VLAN group:

1) Set the VLAN ID;
2) Choose the port members to be assigned to this VLAN group in **Egress Ports** list;
3) The default TAG modes for all port members are **UNTAG Mode**, remove the default option on the specified ports when these ports need to be configured as **TAG** mode;
4) Click **Add** button to create the new VLAN group;
5) Left **VLAN Table** will list all the created VLAN groups;

Change created VLAN groups:

1) Select the VLAN group entry to be changed in **VLAN Group** table;
2) Modify the port members belong to the selected VLAN, or change their **TAG/UNTAG** mode;
3) Click the **Set** button to apply the new VLAN partitions;

Delete created VLAN groups:

1) Select the VLAN group entry to be deleted in **VLAN Group** table;
2) Click **Delete** button to delete the selected VLAN;

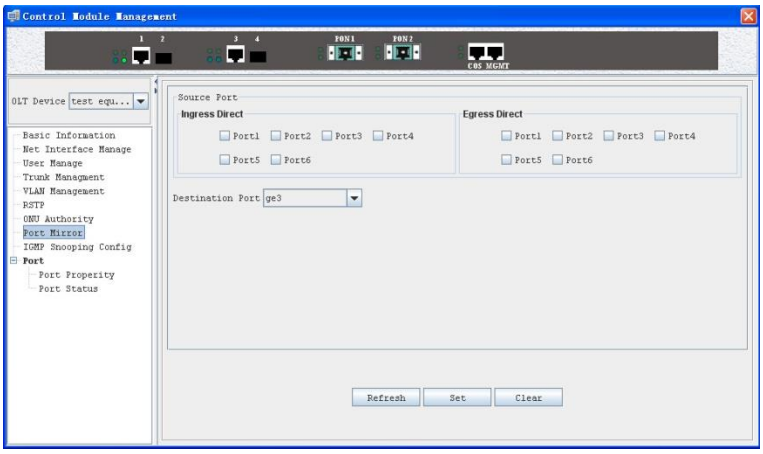
6.2.6 Port Mirroring

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion detection system.

To use the port mirroring feature, you must designate one or more source ports and one destination port. The source ports are the ports whose packets are mirrored and monitored. The destination port is the port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port on the switch.

FD1002S switch engine support port mirroring. All switch ports, including uplink and downlink ports, can be designated as source ports. One of four uplink port can be designated as destination port.

Open "**Port Mirror**" page to configure port mirroring function.



Here are guidelines for setting the port mirroring feature:

1) Select source ports. More than one port can be selected as source ports. You can mirror the ingress traffic, egress traffic or both on the source ports. Port1～Port6 can be source ports.

2) Select destination port. Only one uplink port can be designated as destination port. ge1～ge4 port can be destination port.

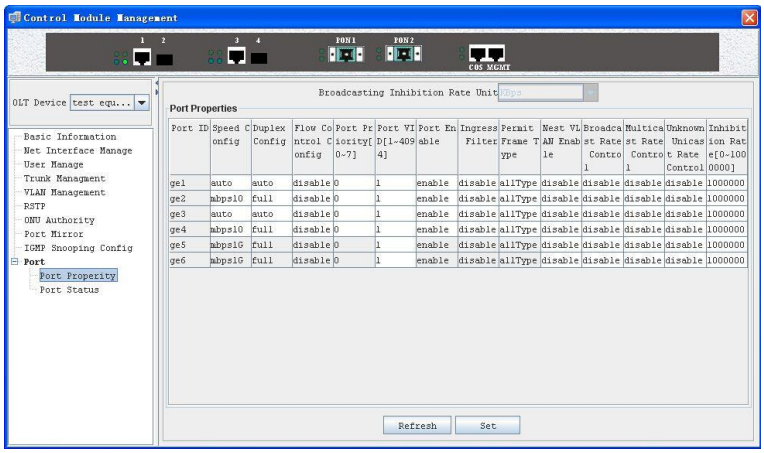
6.2.7 Switch Port Management

This part describes how to display and modify the switch port settings of WDS1U2PGE. The switch ports of FD1002S includes 4 uplink ports (ge1~ge4) and two downlink (connect with PON interface) ports. Fout uplink ports is identified as ge1 to ge4 from uplink port 1 to 4, and two downlink ports is identified as ge5 to ge6 from downlink port 5 to 6.

Open "**Switch and Control Card**" management window. The "**Port Property**" page contains the port configurable parameters and the "**Port Status**" page displays the port working status parameters.

6.2.7.1 Port Property Settings

The port property page typical view is as following figure：



The port list table on this page includes all of the six switch ports. Some parameters are configurable for all ports and some other can only be configured on uplink ports. The parameters displayed as gray style in this table cannot be modified.

Following are the parameters description.

- Port Enable

  Uplink ports can be shut down by setting the **Port Enable** parameter as "**disable**" status. Downlink ports can't be disabled.

- Speed and Duplex

  The speed and duplex mode for uplink ports can be configured. Speed parameter can be set as 10M, 100M and 1000M in "**copper**" mode and fixed

as 1000M in “**fiber**” mode. Duplex mode supports Full Duplex, Half Duplex and Auto Mode.

- Flow Control

  Uplink ports Flow Control mode can be configured as “**enable**”, “**disable**” or “**auto**” mode. The default mode is ‘auto’ mode.

- Port Priority

  The default priority for uplink ports can be modified and the valid range is 0 to 7. The higher value has lower priority.

- Port VID

  All ports default VLAN ID can be modified, and the valid VID range is 1 to 4094.

- Nested VLAN

  Nested VLAN is also called QINQ. When port-based QINQ or protocol-based QINQ is needed on one port, the Nested VLAN mode should be enabled first. All ports support Nested VLAN configuration.

- Broadcast, Multicast and Unknown Unicast Rate Limit

  Uplink ports support rate limit for Broadcast, Multicast and Unknown Unicast traffic. When one of these traffic type is limited, it will be transmitted under the configured rate value. The rate units are **Kbps** and **Kpps** optional.

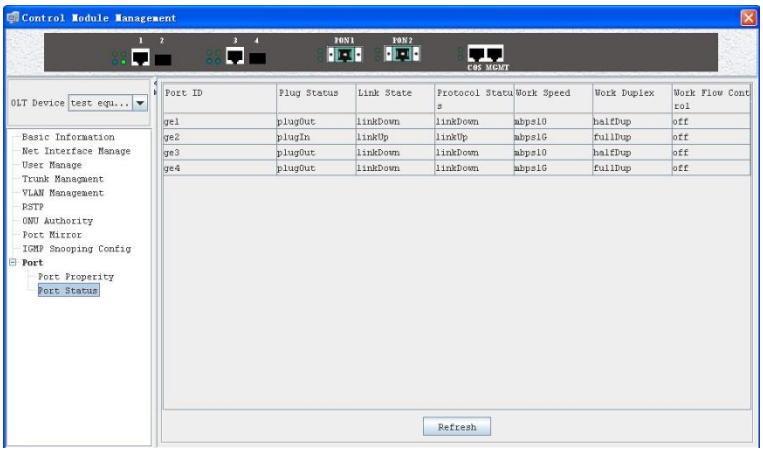
6.2.7.2 Port Status

This page displays the uplink ports working status, including following parameters:

- ✓ Plug Status: SFP transceiver installed or not.
- ✓ Link status, working speed, working duplex mode, flow control mode, and etc.

Parameters displayed on this page can’t be modified.

Following is a typical page view.



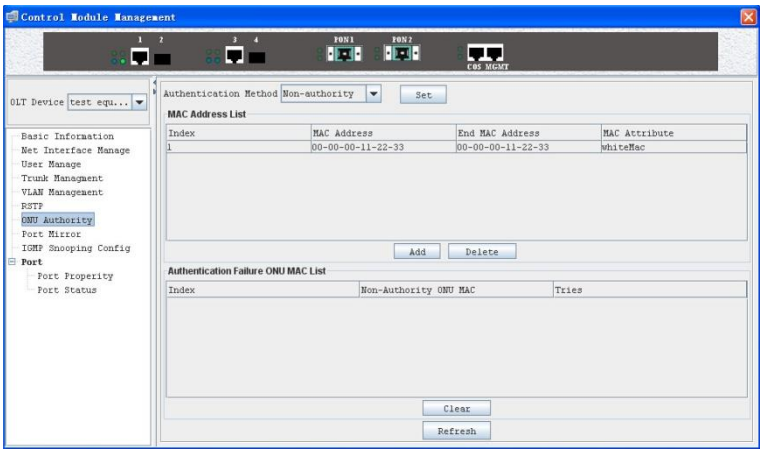
6.2.8 ONU Authentication

WDS1U2PGE device supports authentication feature to accessed ONU devices. Authentication is based on the MAC address of ONU devices and functioned as Black-list or White-list table method. Only one authentication mode can be chosen at the same time.

ONU authentication function is system level feature and the configuration applied to all PON ports of the whole device.

When authentication function is enabled, only those authenticated ONU devices can register to OLT PON ports and others cannot register to OLT PON ports.

Open "**Switch and Control Card Management**" window, into "**ONU Authentication**" page. Following is a typical interface.



To configure the ONU authentication function, perform the following procedure.

1) Choose one authentication mode through the **Authentication Mode** dropdown list.

2) Click **Set** button to enable the chosen mode.

3) Click **Add** button to add a MAC or a MAC range to the "**MAC Address List**" table when the authentication mode is not "**Non-authority**" mode.

4) Click **Delete** button to delete one or more MAC entry from the "**MAC Address List**" table.

Following sections explain the several parts of authentication function.

Authentication Mode

Three authentication modes, "**White List**", "**Black List**" and "**Non-authority**", are supported.

- Non-authority

  When this mode is chosen, ONU authentication function is disabled. That is OLT device will not authenticate the accessed ONU devices. All accessed ONU devices can register to this OLT device. This is also the default authentication mode.

- Black List

  When this mode is chosen, the MAC address whose attributes are "**blackMAC**" will be considered as illegal MACs and the MAC address whose attributes are "**whiteMAC**" will be ignored. The ONUs with illegal MACs will be de-registered by OLT device. The ONUs with MACs that are not included in the Black List can register to this OLT device normally.

- White List

When this mode is chosen, the MAC address whose attributes are "**whiteMAC**" will be considered as legal MACs and the MAC address whose attributes are "**blackMAC**" will be ignored. Only those ONUs with legal MAC can register to this OLT device, and others will be de-registered by this OLT device.

MAC Address List Table

The "**MAC Address List**" table will be checked to judge if a MAC is legal or illegal, when the authentication mode is enabled (Black List mode or White List mode). User can add a unique MAC Address or a MAC Address range to this table by **Add** operation. When do add operation, "Begin MAC" and "End MAC" should be input. A unique MAC will be added if the two MAC Addresses are the same. When add a MAC Address range, the "End MAC" value should be different with the "Begin MAC". Note that the "End MAC" value should be numerical larger than the "Begin MAC" value.

When add a MAC entry, the "blackMAC" or "whiteMAC" attribute should be chosen to logically assign this entry to **Black List** table or **White List** table.

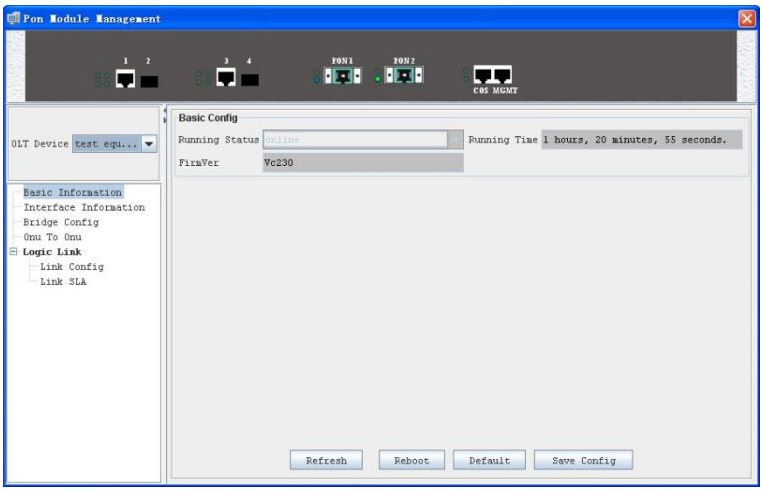
Authentication Failure ONU MAC List Table

This read-only table contains the illegal ONU register information, when authentication function is enabled. Such as the illegal ONUs MAC Address and their number of times try to register. This table contents can be cleared by click **Clear** button.

6.3 PON Card Management

This section describes the management functions of EMS software to manage WDS1U2PGE OLT device. Currently, WDS1U2PGE have two PON ports.

Double click the PON card icons in topology tree or the PON card graphic in chassis management window to open the "**PON Card Management**" window. Following is a typical page view.



6.3.1 Basic Information View

Open "Basic Information" windows, it displays the PON Card firmware version, Running Time, and Running Status etc.

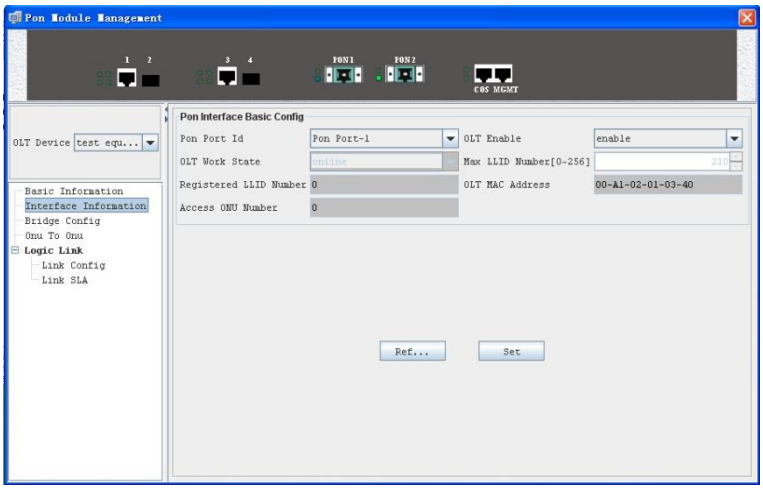
The led indicators located on the front panel graphic display the PON module's real time working status. There are two LED on the left of the PON port, are indicator of status of ONU connecter with the PON port.

6.3.2 Basic Operation

On "Basic Information" page, user can reset the card, default the card to factory configuration or save the configurations by click the corresponding operation button.

6.3.3 OLT Management

Open 'OLT Management' page，following is a typical page view:



On this page, user can do the following operations:

- OLT Enable/Disable

  Enable or disable the PON ports of this PON card. When the PON ports are disabled, all ONUs registered on this card will be de-registered. Note that some other configurations can only be modified when the PON ports are disabled.

- Max LLID Number

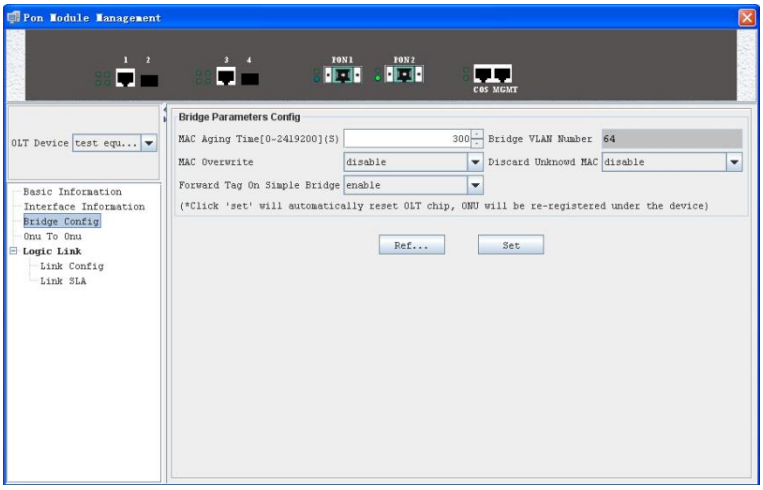
  This parameter is the max LLID number allowed to register for per PON port. One ONU device may register one or more LLID to the connected PON port. This parameter can only be modified when the PON port is disabled.

- LLID/ONU Registered Number

  These parameters display the registered LLID number and the registered online ONU device number for per PON port.

6.3.4 OLT Bridge Configuration

Open “Bridge Configuration” page, user can modify the following bridge parameter settings:



- MAC Aging Time

The aging time for MAC Address learned on PON ports. The valid value range is 0 to 2419200 seconds. When this value is 0, the MAC aging feature is disabled. The default value is 300s.

- MAC Overwrite

When this function is enabled, and the dynamic MAC table is full, new learned MAC Address will overwrite the oldest MAC entries.

- Discard Unknown MAC

When this function is enabled, the bridge engine will not forward unknown unicast packets.

- Forward TAG Frame on Simple Bridge

When this function is enabled, the bridge engine will forward all tag and untagged frames. When this function is disabled, the bridge engine will forward only untagged frames.

Note:

1) *All the above parameters can only be modified when the PON ports are disabled.*
2) *EMS software will disable all PON ports first automatically when modify the above parameters, and then enable them when finished.*

6.3.5 ONU P2P

Due to the nature of the EPON network structure, the ONU device registered on the same PON port cannot communicate with each other. This feature will affect some special application. If the communication is required, the P2P (point to point) function must be enabled.

On the "**P2P Configuration**" page, user can enable or disable this function.

Note:

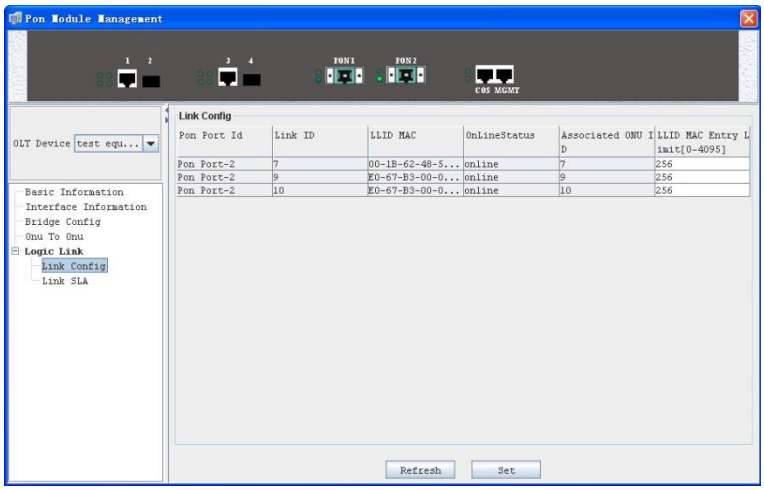
1) *This configuration can only be modified when the PON ports are disabled.*
2) *When change this configuration, EMS software will shutdown the PON ports first, and then open them when change finished.*
3) *According to IEEE802.3 protocol, the point to point operation between ONUs of the same PON port is not supported, so we do not recommend users to enable this function, unless it is really needed.*

6.3.6 LLID

6.3.6.1 Configuring LLID

Each ONU can register and get one or more LLID in EPON system. We can control the number of users under each logic link (by MAC restrict) .

Click 'Logic Link'->'Link Configuring'：



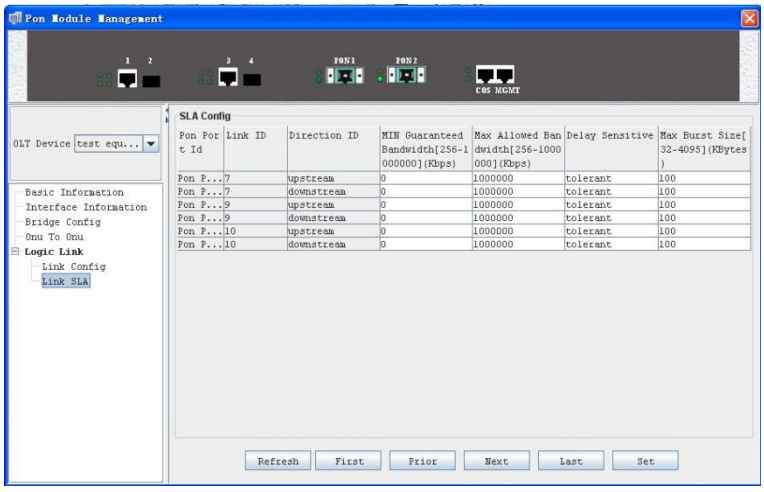
Default MAC limit is 64，so each Logic Link can service to 64 user simultaneously. Number of concurrent users can be configured from 0 to 4095.

6.3.6.2 Configuring Logic Link SLA

SLA refers to the Service Level Agreement. In EPON system, OLT device maintain a SLA configuration for each registered Logical Link. SLA configurations include minimum guaranteed bandwidth, maximum allowed bandwidth, delay sensitive, and maximum burst size parameters.

By configuring different SLA parameters, EPON system can allocate different service levels for different customers based on their service demands.

Click ‘Logic Link’->‘Link SLA’ ：



As above figure, SLA configurations for each PON port, Logical Link ID and Direction are listed in the “SLA Configuration” table. Logical Link ID is assigned

by OLT device when ONU registered to it.

SLA parameters are introduced as following:

- Minimum Guaranteed Bandwidth

  Also called assured bandwidth, is the bandwidth that OLT will allocate to this Logical Link assuredly. The valid value range is 0 to 1000000, unit is kbps. The default value is 0.

  Note: *Total minimum guaranteed bandwidth for all Logical Links registered to per PON port can't exceed the max throughput value. Normally, it is 950Mbps on downlink direction and 930Mbps on uplink direction. When exceed, the guaranteed bandwidth may be not effective.*

- Maximum Allowed Bandwidth

  Maximum allowed bandwidth is also called best effort bandwidth. It is the maximum bandwidth that OLT can allocate to one Logical Link when there is free bandwidth. The valid value range is 0 to 1000000, unit is kbps. The default value is 1000000.

- Delay Sensitive

  This parameter can be set as "tolerant" or "sensitive". The "sensitive" option can only be set when the maximum allowed bandwidth is equal to the minimum guaranteed bandwidth. Under this configuration, the Logical Link will have lower delay performance.

- Max Burst Size

  The maximum allowed burst frame length on this Logical Link. The valid range is 1 to 256, unit is Kbytes. The default value is 100. The default value is recommended.

Note:

1) *User can also view or modify the SLA configurations on "Logical Link-Link SLA" page on "ONU Management" window. They have the same configuration results.*
2) *It is convenient to modify the configurations on "ONU management" page for per ONU device and have a whole view on "PON card management" page.*

7 ONU Management

7.1 ONU Management Introduction

ONU is the user end device in EPON system. EMS software manages the accessed ONU devices through their registered OLT device. OLT device transmits

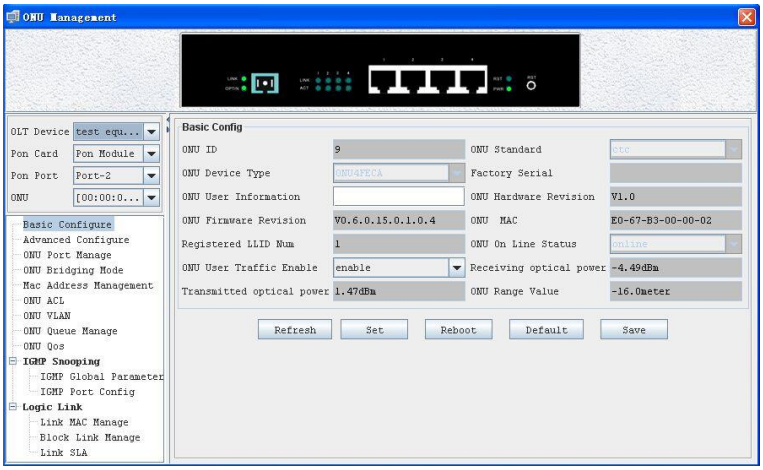
management operations received from EMS software to accessed ONUs through OAM frames defined based on IEEE802.3ah standard.

EMS software supports to manage various types ONU devices, such as 1FE port type, 4FE port type, 4FE+2POTS type and 4FE+2POTS+1CATV type, etc, as long as these ONU devices support standard OAM features.

This part introduces the management operations for EMS software to manage 4FE-port type ONU device. For other types, the mainly operations are the same and different management features are introduced in their special sections.

Double click the selected ONU device icon on topology-tree list to open “ONU Management” window. The function pages located on this window contain all the management features for this type ONU device.

Following is a typical interface view for ONU management.



As above figure, a typical type ONU device supports following main management features.

- ONU Basic Device Information
- ONU Basic Operation
- RSTP Configuration
- ONU User Port Management
- ONU Bridge Configuration
- ONU MAC Address
- ONU Loopback Test
- ONU IGMP Snooping
- ACL Configuration
- VLAN Management

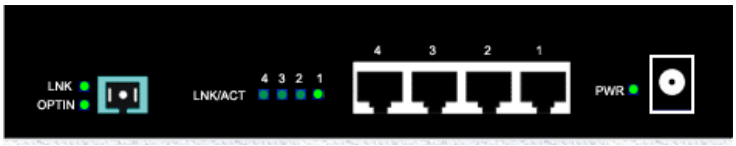
- ONU Queue Configuration
- ONU Port Ingress Policing, Egress Shaping
- ONU Logical Link SLA Configuration

Following sections introduce these ONU management features.

7.2 ONU Basic Information

7.2.1 LED Indicator

Usually, the device panel diagram will be displayed on the ONU management window. On this diagram, all the working LED indicators show the actual working status. See the following example figure.



The bright green icon indicates light ON and the dark LED icon indicates light OFF.

7.2.2 Basic Information

Open “Basic Configure” page, the ONU basic information is displayed on this page.

On this page, user can view device type, MAC Address, ONU ID Number, Device SN, Hardware Revision, Firmware Version, User Information, Max Allowed LLID Number, Online Status and Range Value etc.

Following are explanations for some special parameters.

- ONU ID

ONU ID is the ONU device ID number which is assigned by OLT device. ONU ID is convent for user to identify per ONU device. ONU ID is a unique value for per PON port, the range is 1 to 64. When an ONU device registered to a PON port, OLT assigned an unused ONU ID value for it. This value will be bound with the ONU’s MAC Address until the ONU device is deleted from this PON port (can only be deleted when offline). When an ONU device is deleted from one PON port, the ONU ID value assigned for it will be taken back. When the deleted ONU registered to this PON port again, it will be assigned a random new ONU ID value.

- MAX Allowed LLID Number

Some types ONU device support multiple LLID, for these types device, user can configure the maximum allowed LLID number for it. For OLT device, one LLID is considered as a virtual ONU.

- Registered LLID Number

This parameter is the LLID number registered to OLT device currently.

- User Information

This parameter is used for user to fill user special information for per ONU device.

- Range Value

This parameter is the optical link distance from OLT to ONU device measured by OLT device.

7.2.3 Basic Operation

Open “Basic Configure” page. User can do Reset, Default and Save operation for per ONU device through the function buttons located on this page.
Through the “User Traffic Enable” function, user can enable or disable the service traffic transmission.

7.3 RSTP Configure and Port Isolation

Open “Advanced Configure” page. Following is a typical figure.

RSTP

The Rapid Spanning Tree Protocol (RSTP) guard against the formation of loops in an Ethernet network topology. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.
The ONU RSTP function applies on ONU user ports, used to prevent network loop on these ports. When network loop occur, such as two user ports are connected mistakenly, one of them will be shutdown automatically by STP protocol.

By setting “**RSTP**” parameter “enable/disable”, RSTP function can be turned on or off.

Port Isolation

For multiple user ports ONU equipments, Layer 2 switch among these ports is supported usually. But for most access network build based on EPON technology, the communication among local users is not needed in most case. The network designer can turn on or off switch capability among ONU user ports by setting “Port Isolation” parameter “enable/disable”.

7.4 ONU Port Management

This section describes the management function and parameter configuration for ONU user ports.

ONU user port management includes the following:

- Port Working Status
- Port Bridge Mode Configuration
- Port MAC Address List
- Ingress Policy and Egress Shaping

The following subsections introduce the above content.

7.4.1 Port Working Status

Open “ONU Port Management” page. Typical page is shown below.

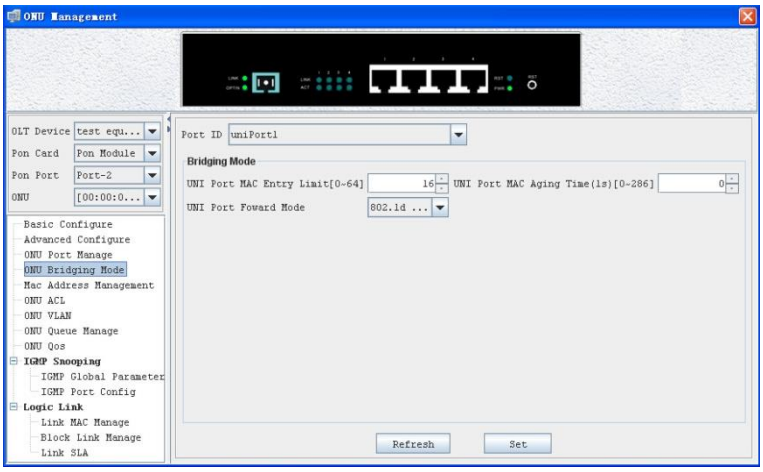
Link Status, Speed and Duplex Working Status, Flow Control, Port Enable Status and User Information parameters for all user ports can be viewed on this page.

Port Speed and Duplex working mode, User Information for per Port, Flow Control and Port Enable parameters can be configured on this page.

Port Speed and Duplex parameters can be configured only when the port is enabled and port link status is Up and Auto negotiation is disabled.

7.4.2 Port Bridge Mode

Open “ONU Bridge Mode” page. Typical page is shown below.



Bridge mode parameters for per ONU port can be configured on this page. These parameters include MAC Limit, MAC Aging Time and Forwarding Mode etc.

MAC Limit

This parameter is used for network manager to control the maximum learned MAC Address entries.

When the forwarding mode is “dropUntilLearned”, the new received packets with un-learned MAC Address will be dropped when the number of learned MAC Address come to the configured MAC limit value. When the forwarding mode is configured as “d8021mode”, the new received packets will be flooded to all ports and their source MAC will not be learned when the number of learned MAC Address come to the configured MAC limit value.

Forwarding Mode

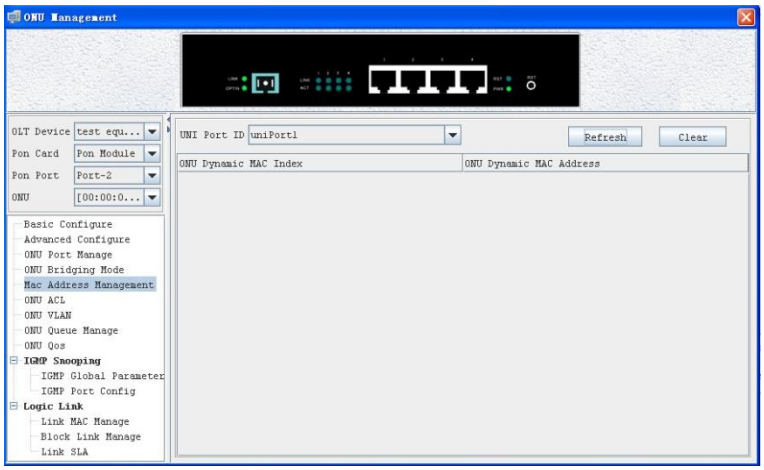
The ONU user port forwarding mode can be configured as “drop until learned” mode and “802.1d” mode by setting this parameter value as “dropUntilLearned” or “d8021mode”. When the forwarding mode is “drop until learned” mode, only the packets with learned source MAC Address will be forwarded, the un-learned packets will be dropped. In “802.1d” mode, all received packets will be forwarded based on 802.1d standard.

MAC Aging Time

MAC Aging time can be configured for per user port, it is the aging time for dynamic MAC Address entries in MAC Address table. The value unit is second. When this value is set to 0, the learned MAC Address entries will not be aged out.

7.4.3 MAC Address Management

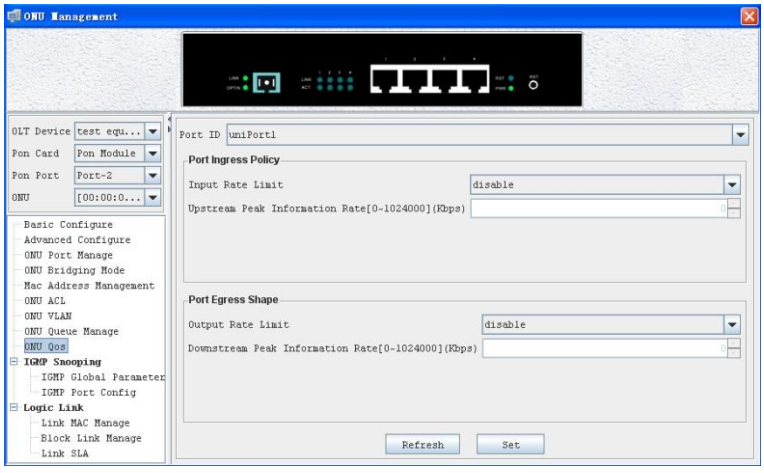
Open “MAC Address Management” page, manager can view the learned dynamic MAC Address entries on each user port. Click **Clear** button to clear.



7.4.4 Ingress Policy and Egress Shaping

ONU user ports support traffic management feature on both up and down direction. Upstream direction (received on user port) traffic supports ingress policy feature and downstream direction traffic supports egress shaping feature.

Open “ONU Qos” page, typical page is shown below.



Ingress policy feature supports to configure the maximum data rate received on

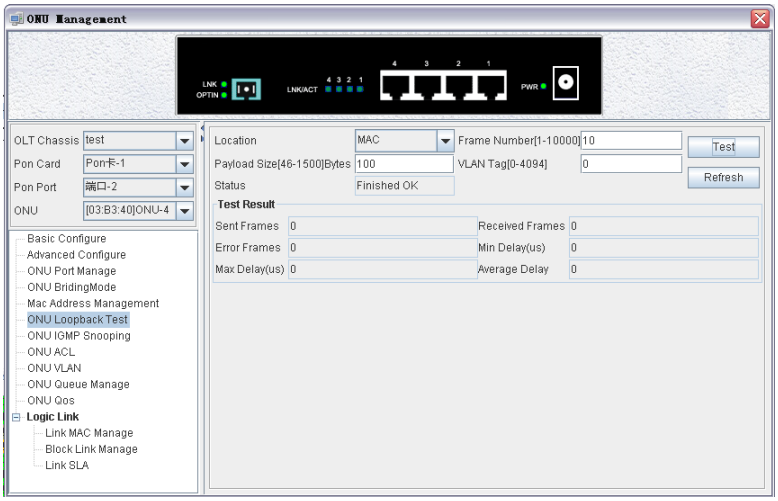
each user port based on selected packet type. The packet types to apply ingress policy feature can be broadcast packet, multicast packet, all packets and broadcast/multicast/DLF packets. The rate unit is kbps and maximum value is 100000kbps. The ingress policy feature can be disabled.

Egress shaping feature supports to configure the maximum output data rate on each user port. And the rate limit mechanism can be “weight fair” or “strict priority”.

7.5 ONU Loopback Test

Loopback test function is used for network manager to test network performance between OLT and ONU equipment. When do loopback test operation, test packets are sent to target ONU device from OLT PON port and then these test packets are looped back to OLT PON port by the ONU device. OLT software will compare the received test packets with the packets sent from it to get the test results, such as sent and received packets, error packets and delay performance. Network performance on the test optical link can be evaluated based on the loopback test results.

Open the “ONU Loopback Test” page. Typical page is shown below.



Loopback test steps are as follows:

1) Before beginning loopback test, test packet number, frame length and VLAN TAG should be set first. Set VLAN TAG as 0 indicates sent un-tag frames.

2) Choose loopback location, “MAC” or “PHY” can be chosen. This option is used to specify from which the test packets will be looped.

3) Click **Test** button to start test.

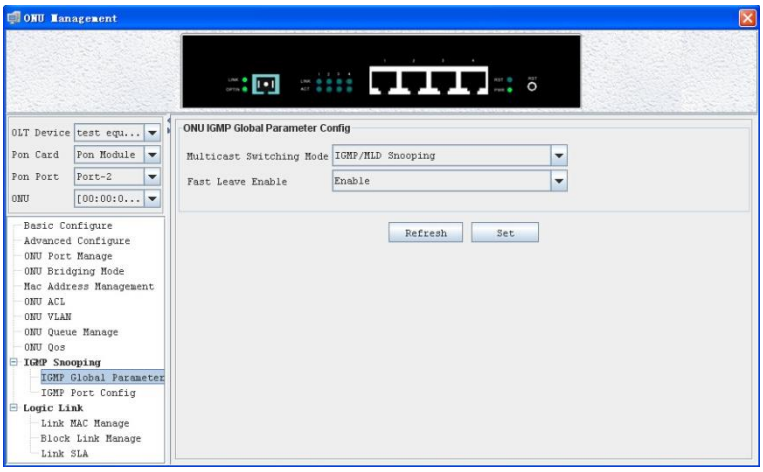
4) When test finished, the test results will be shown on the result table.

7.6 ONU IGMP Snooping

IGMP snooping can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP Multicast Routers/Switches and IP Multicast hosts to learn the IP Multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

ONU maintains a table of relationship between a multicast MAC address and ONU ports. When an ONU port receives a Host Membership Report message, ONU join this port to the corresponding table entry. When the ONU receive a multicast packet, ONU check this table to determine which ports to forward this packet.

IGMP global parameters include "multicast switching mode" and "fast leave enable". The following figure shows the "ONU IGMP Global Parameter Configure" Page.



ONU device supports five different "Multicast Switching" modes:

- IGMP/MLD Snooping Mode

This mode is IGMP Snooping and MLD dual modes.

- CTC Controllable IGMP/MLD Mode

This mode is Host controllable mode for IPv4 and IPv6 multicast.

- IGMP Snooping Mode

This mode is IGMP snooping only mode.

- CTC Controllable IGMP/MLD Mode

This mode is Host controllable mode for IPv4 multicast.

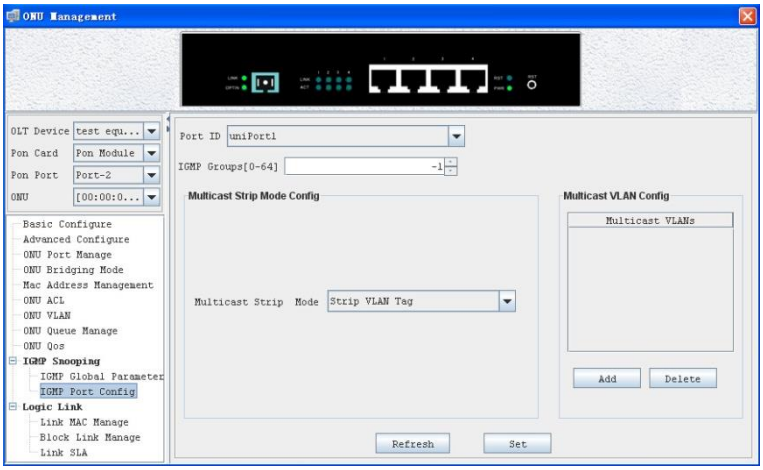
- Path Through Mode

This mode is all IGMP/IPMC/MLD/IPv6 Multicast are passed through mode.

Fast Leave Enable

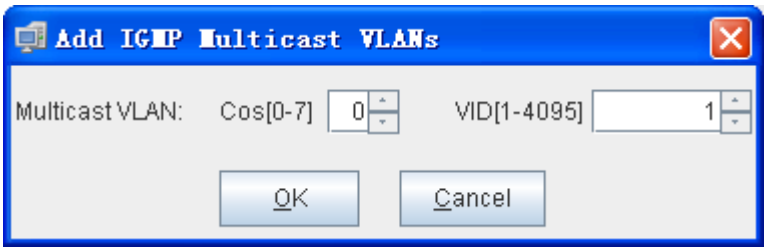
When Fast Leave is enabled, forwarding of a group stops immediately upon reception of a Leave message for that group. Note that this feature is only useful if it is known that exactly one device downstream of the ONU can join a group. If more than one device is attached to the ONU port though a switch or hub, then the first one to leave would stop traffic to both devices.

The following figure shows the “IGMP Port Configure” Page.



"IGMP Group" is used to configure how many multicast groups this ONU port can join in.

Click **Add** button on the "Multicast VLAN Configure" Panel to open the "Add IGMP Multicast VLANs" window, as shown in the following figure:



Enter the Cos and the VID then click **OK** button to add a multicast group to this ONU port, after that multicast streams contains this multicast VLAN Tag will be transmitted to this port. Because the port receives a multicast stream with a VLAN Tag, so you will need to configure the multicast VLAN Tag processing mode.

ONU supports three different VLAN tag processing mode: **Not Strip VLAN Tag**, **Strip VLAN Tag** and **Switch VLAN Tag**。

- Not Strip VLAN Tag

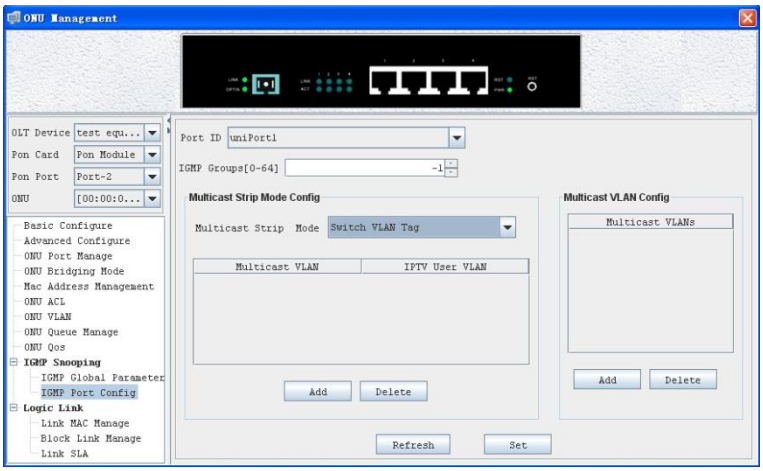
Do not strip the VLAN Tag in the multicast stream. Multicast stream sent from this port still contains a multicast VLAN Tag.

- Strip VLAN Tag

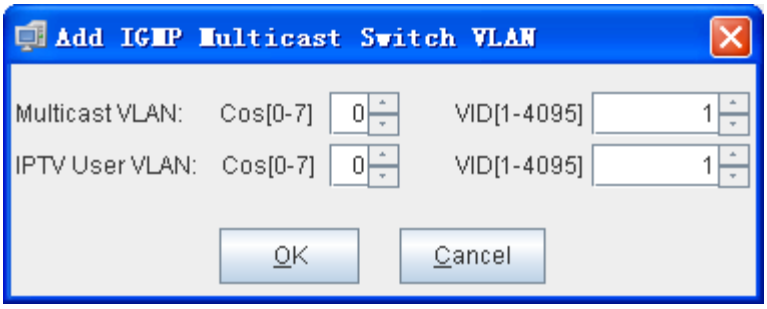
Strip the VLAN Tag in the multicast stream. Multicast stream sent from this port does not contain a multicast VLAN Tag.

- Switch VLAN Tag

Overwrite the VLAN Tag in the multicast packet then forward. This mode configuration page as shown in the following figure:



Click **Add** button on the "Multicast Strip Mode Configure" panel to open the "Add IGMP Multicast VLANs" window, as shown in the following figure:

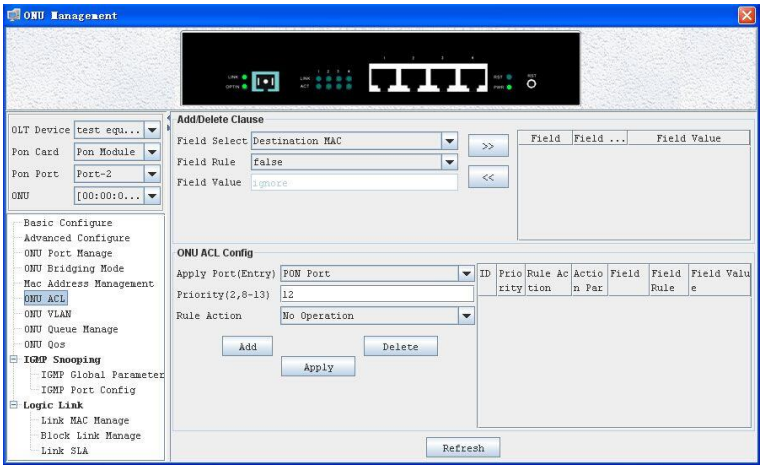


"**Multicast VLAN**" parameter is used to match VLAN Tag in the multicast streams. When the VLAN Tag of the multicast streams is equal to this "Multicast VLAN", ONU overwrite the VLAN Tag of the multicast with "IPTV User VLAN" then forward.

7.7 ONU ACL Configuration

ACL(Access Control List) using packet filtering, read the Ethernet frame header information such as source address, destination address, source port, destination port, and so on, forward or filter the packet according to the predefined rules, so as to achieve the purposes of access control.

The following figure shows the "ACL configuration" Page.



To configure an ACL rule, follow these steps:

Step 1: define the matching conditions

A matching condition consists of one or several (up to 8) matching rules. These matching rules are "and" relationship, namely only when all the rules are established, the matching condition is established.

A matching rule consists of the following components:

Matching fields: A matching field is a continuous series of bits in a frame, such as destination MAC address, source MAC, LLID, Ethernet frame type, VLAN ID, COS priority, IP protocol type, L4 source port, L4 destination port, TOS priority, source IP address, destination IP address.

Rule operators: Rule operators compare the value of rule field in the incoming frame with a specified value. The result is a Boolean value, either true or false. 8 of the following Rule operators are supported:

Symbol	Description
false	Always FALSE; Never match
==	Field Equal to value
!=	Field Not equal to value
<=	Field Less than or equal to value
>=	Field Greater than or equal to value
exist	True if field exists
!exist	True if field does not exist
true	Always TRUE; Always match

Matching value: The matching value is the value which specified by user used in the bool comparison in a clause.

Click the "**>>**" button to add the matching rule to the rules list.

Click the "**<<**" button to remove the selected rule in the rules list.

Step 2: specify the target port of the matching condition

ACL rule can be applied to ONU PON port or UNI port. If an ACL is applied to PON ports, then this ACL rule take effect for downstream packets. If an ACL is applied to UNI ports, then this ACL rule take effect for upstream packets.

Step3: Specify rule precedence

The defined range of precedence for user rules is from 8...13. 8 has the highest precedence.

Two rules with conflicting actions may match the same frame. In this case, the action of the rule with the highest precedence (lowest numerical value) is applied to the frame. The action from the lower precedence rule is ignored.

Step 4: Specify action categories

When an Ethernet packet matches one or more ACL rules, it will be filtered or forward according to the rule category.

Action categories can be forward or discard a frame, set the Destination queue for a frame, delete an existing VLAN tag, add a new VLAN tag, set VID, set CoS, and so on.

Step 5: Apply

Set up the ACL rule, click on the "**Add"** button to add the ACL rule to the ACL rule lists.

Click **Delete** button to delete the selected ACL rule entry.

Click **Apply** button to apply all rules in the ACL rule list to the ONU.

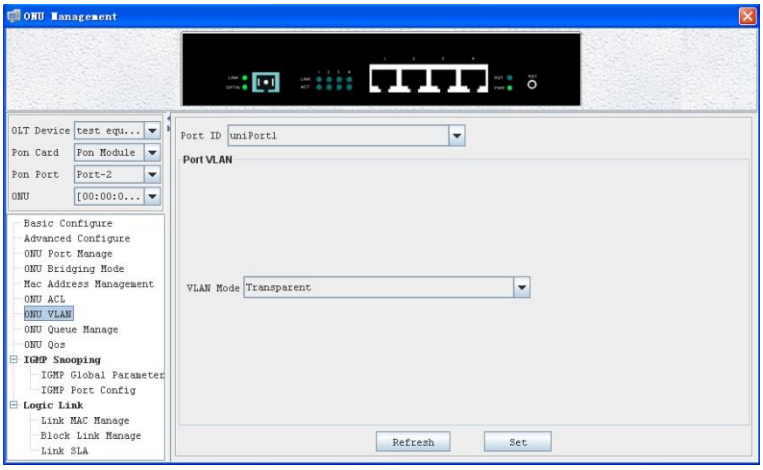
7.8 ONU VLAN Configuration

ONU supports four port VLAN modes: **Transparent** mode, **Tag** mode, **Translate** mode, **Trunk** mode. These four modes are introduced as follows:

Transparent Mode

In this mode, upstream or downstream Ethernet packet received at this ONU port forward without processing.

The following figure shows the Transparent VLAN configuration Page.



Refresh button: refresh the Port VLAN configuration.

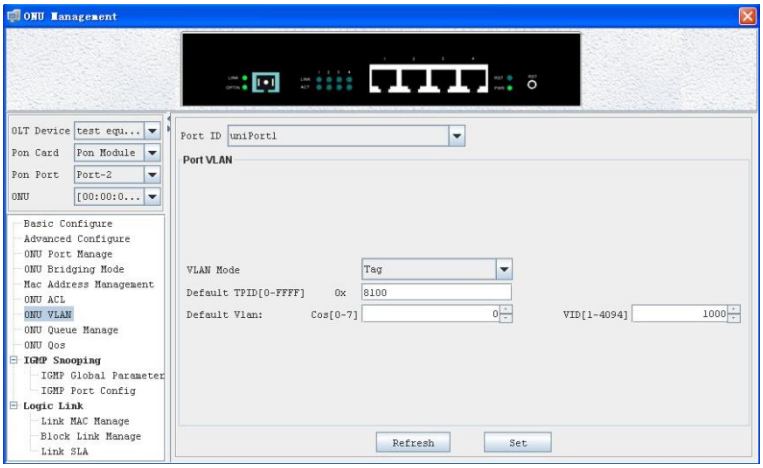
Set button: apply the port VLAN configuration to this ONU port.

Tag Mode

The method of an ONU port under tag mode process an Ethernet packet is shown in the following table:

Direction	With VLAN Tag	Operation
Upstream	Yes	Discard this packet
	No	Add default VLAN Tag to this packet and forward.
Downstream	Yes	If the VID is not equal to the port default VLAN ID, discard this packet. Otherwise strip the VLAN Tag of this packet and forward.
	No	Discard this packet

The following figure shows the Tag VLAN configuration Page.



Refresh button: refresh the Port VLAN configuration.

Set button: apply the port VLAN configuration to this ONU port.

Translate Mode

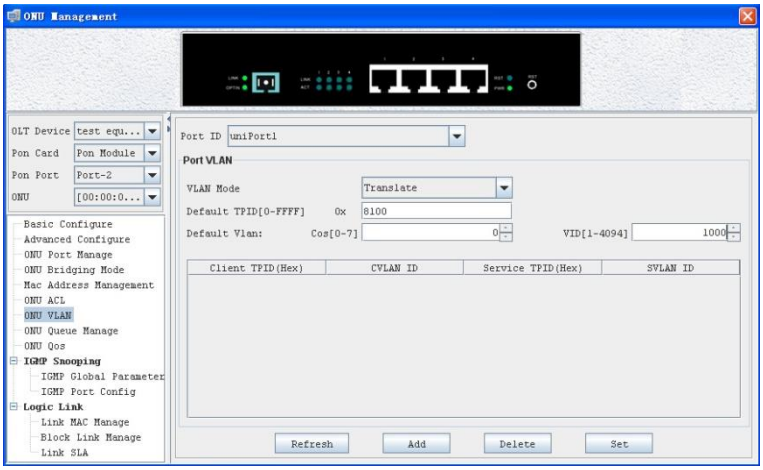
Translate mode allows the port overwrites VLAN tag.

The method of an ONU port under trunk mode process an Ethernet packet is shown in the following table:

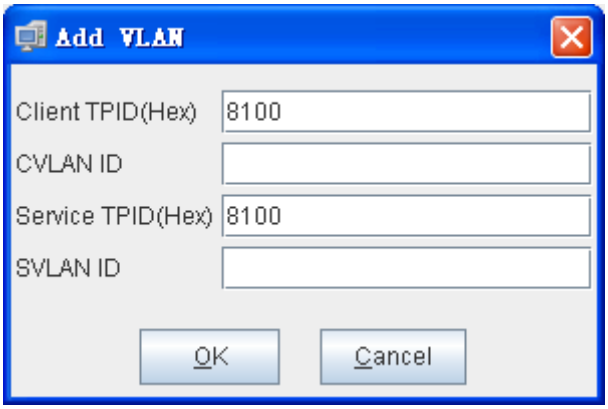
Direction	With VLAN Tag	Operation
Upstream	yes	If the VID of a packet equal to the CVLAN ID of a certain translation entry, overwrite the packet's VID with this entry's SVLAN ID and forward this packet; If the VID of a packet is not equal to any translation entry's CVLAN ID, discard this packet.
	no	Add default VLAN Tag to this packet and forward this packet.
Downstream	yes	If the VID of a packet equal to the SVLAN ID of a certain translation entry, overwrite the packet's VID with this entry's CVLAN ID and forward this packet; If the VID of a packet is not equal to any translation entry's SVLAN ID, discard this packet.

	no	Discard this packet.

The following figure shows the Translate VLAN configuration Page.



Add button: add Translate entry. Click **Add** to open the **Add VLAN** window, shown as below:



Click **OK** button after input the TPID and VID, a new translate entry will be added to the VLAN Translate list. Up to 8 VLAN translate entry can be set for an ONU port.

Delete button: delete a VLAN translate entry selected in the VLAN Translate list.

Refresh button: refresh the Port VLAN configuration.

Set button: apply the port VLAN configuration to this ONU port.

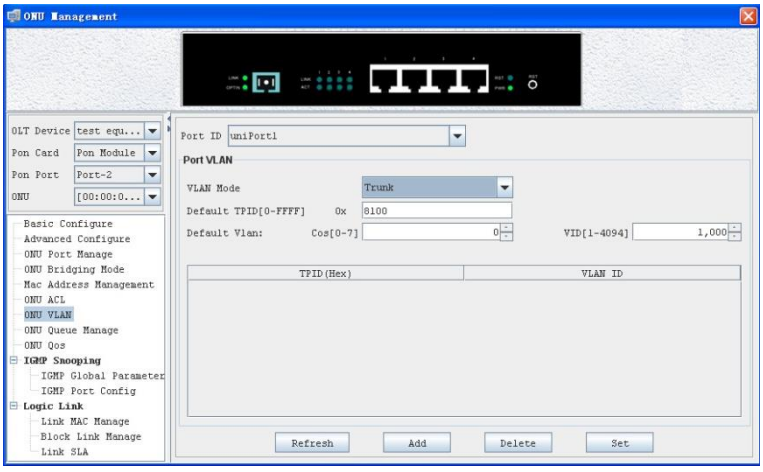
Trunk Mode

Trunk mode allows the port forward multiple VLANs at the same time, generally used for the connection between the network equipment.

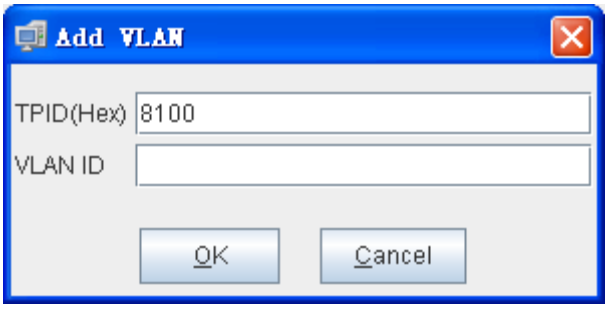
The method of an ONU port under trunk mode process an Ethernet packet is shown in the following table:

Direction	With VLAN Tag	Operation
Upstream	yes	If the packet's VID exist in the VLAN Trunk allow list or equal to the port default VLAN ID, forward this packet, otherwise discard this packet.
	no	Add default VLAN Tag to this packet and forward this packet.
Downstream	yes	If the packet's VID equal to the port default VID, strip the VLAN Tag of this packet and forward this packet. If the packet's VID not equal to the port default VID but exist in the VLAN Trunk allow list, forward this packet. If the packet's VID not equal to the port default VID and not exist in the VLAN Trunk allow list, discard this packet.
	no	Discard this packet.

The following figure shows the Trunk VLAN configuration Page.



Add button: add allowed VLANs. Click **Add** to open the **Add VLAN** window, shown as below:



Click **OK** button after input the TPID and VID, a new entry will be added to the VLAN Trunk allow list. Up to 16 allow VLAN entry can be set for this ONU port.

Delete button: delete a VLAN entry selected in the ONU VLAN list.

Refresh button: refresh the Port VLAN configuration.

Set button: apply the port VLAN configuration to this ONU port.

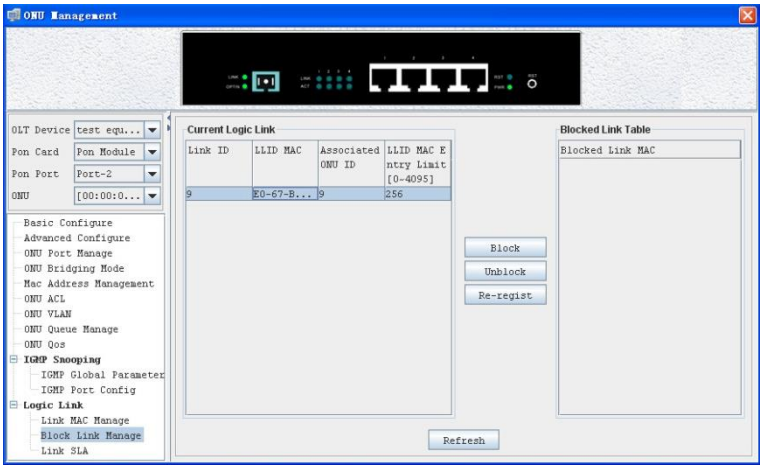
7.9 ONU Logical Link Management

Based on EPON protocol standard, OLT equipment will allocate one or more Logical Link for each successfully registered ONU device. The Logical Link is also called LLID simply. In downstream direction, OLT add LLID field to the received standard Ethernet frames and then sent them to all registered ONU devices. ONU device will only receive the frames with the same LLID value as the one it registered. In upstream direction, OLT schedule and manage upstream packets based on the Logical Links registered by ONU devices.

Open “ONU Management” window and go to “Logical Link” page to do Logical Link management. Following subsections introduces the Logical Link management features.

7.9.1 Logical Link Status Management

Open “Logical Link Status Management” page. Typical page is shown below.

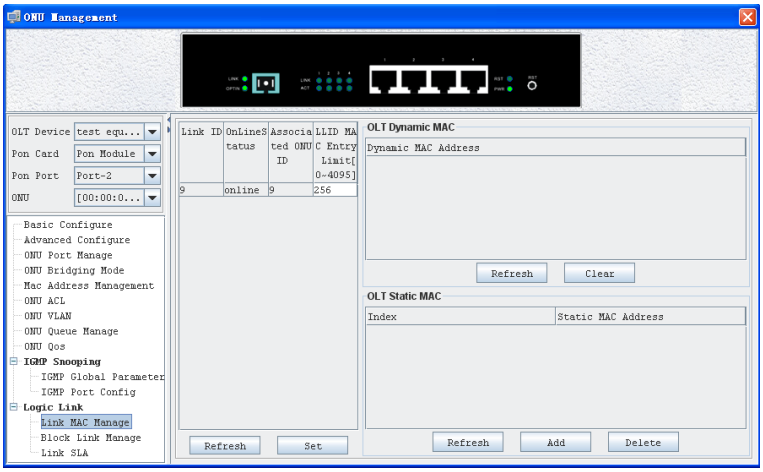


The “Current Logical Link” table shows all the Logical Links registered by this ONU device. Each Logical Link is identified by its MAC Address. The **Block** and **Unblock** button is used to block or unblock Logical Links. The **Re-register** button is used to force a Logical Link to reregister to OLT.

When a Logical Link is blocked, it will be deregistered and can’t reregister again until it is unblocked later.

7.9.2 Logical Link MAC Address Management

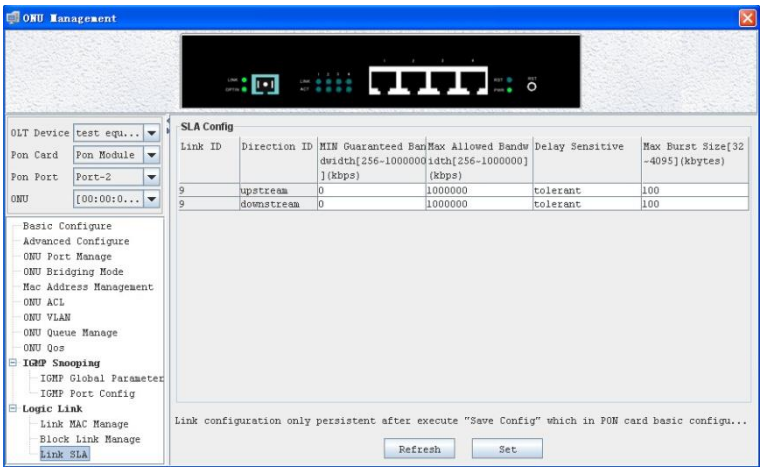
Open “Logical Link-Link MAC Management” page, typical page is shown below.



On this page, network manager can view or clear dynamic MAC Address entries learned on each Logical Link. Can add or delete static MAC Address entries on each Logical Link.

Logical Link MAC Address tables are maintained on OLT device. OLT forwards downstream frames based on MAC Address table.

7.9.3 Logical Link SLA Management



Open “Logical Link-Link SLA” page. Typical page is shown below.

On this page, network manager can configure SLA parameters for the Logical Links registered by this ONU device.

The Logical Link SLA management features here are accordant with the SLA configurations introduced in PON card management section. Please refer to subsection for detail introduction.

8 Alarm Management

This chapter introduces EMS alarm management features.

EMS software receives alarm information sent from managed EPON equipments. The alarm information is contained in TRAP messages based on SNMP protocol standard. To receive TRAP messages sent from managed device, target IP Address should be configured first. The target IP Address is the PC server’s IP Address on which EMS software is installed. Please refer to section to learn the operations to configure these parameters.

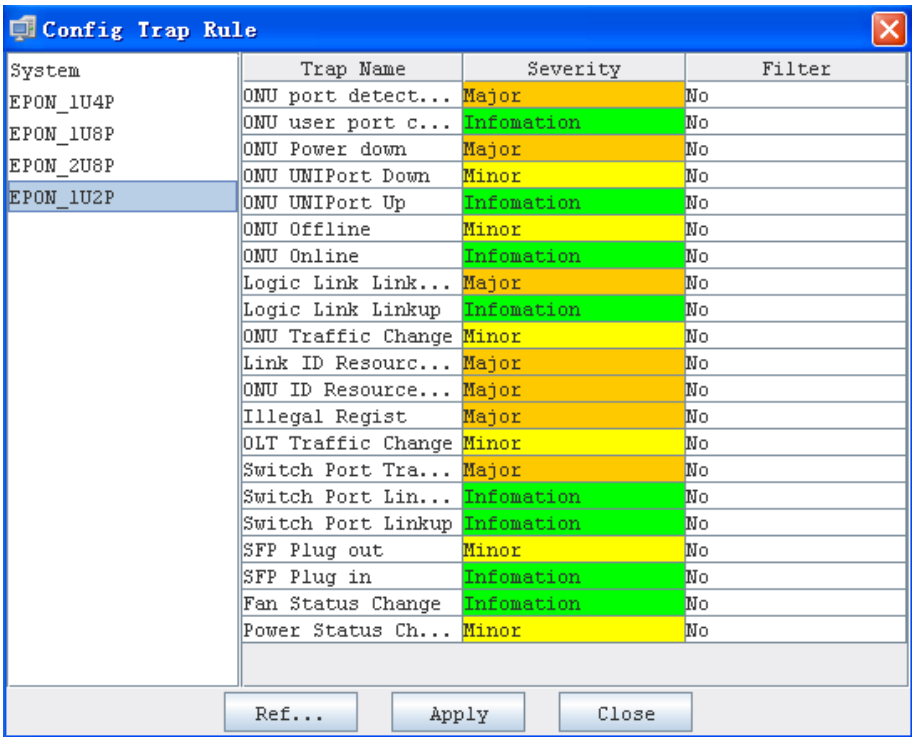
EMS software supports user defined alarm rule configuration. Based on defined rule, alarm information can be classified or filtered.

Network manager can query current alarm and history alarm information occurred on managed equipments by various search conditions.

Following sections introduce the alarm management details.

8.1 Alarm Rule Configuration

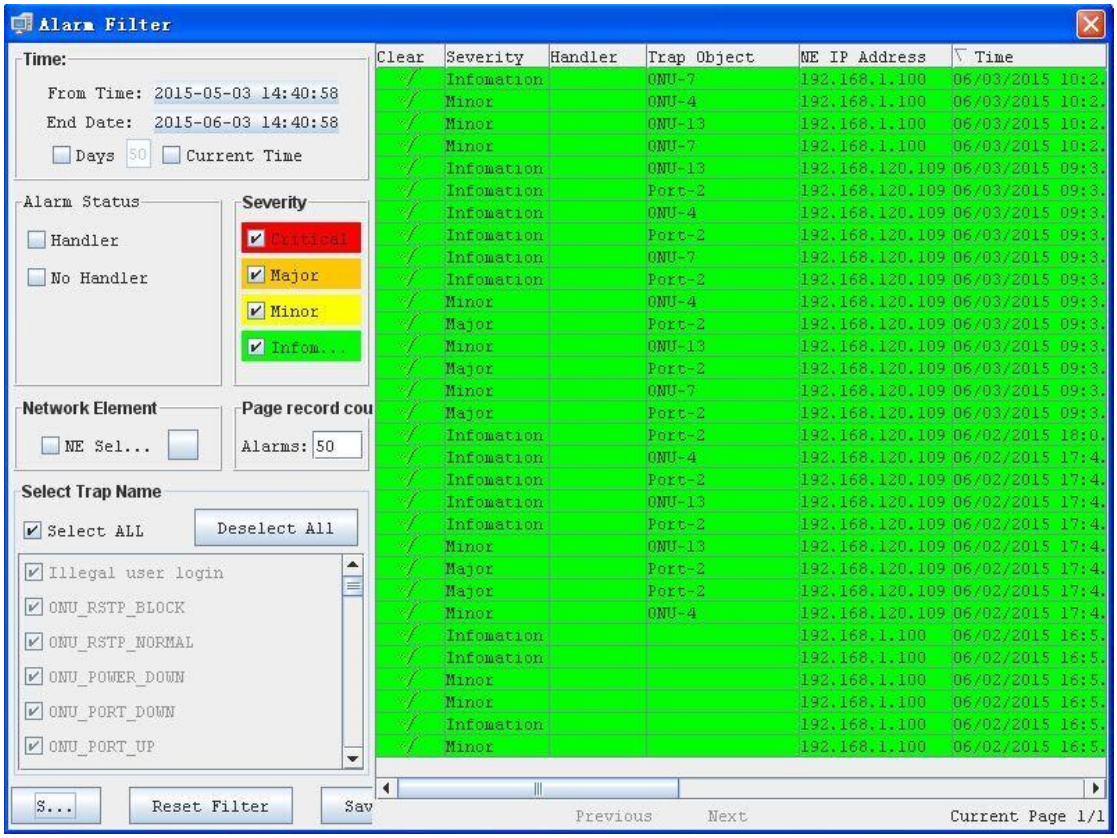
To open “Alarm Rule Configuration” window, from Alarm menu, then click Alarm Rule Configuration. Following figure is a typical view.



Choose the target device type in left column, such as “EPON_1U” OLT device. Then the supported alarm items for the selected type will be shown on right part. Each entry contains the alarm name, severity level and filter or not. Severity level is configurable and classified as “**Information**”, “**Minor**”, “**Major**” and “**Critical**” four levels. Different level alarms will be marked with different color in alarm window. Any one of the supported alarm items can be filtered out according to requirement.

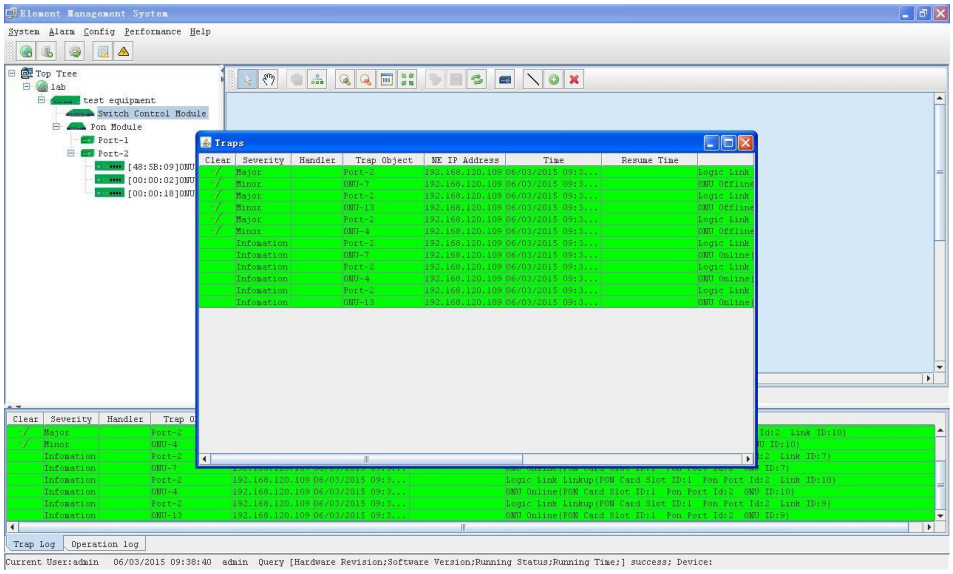
8.2 Alarm Query

To open “Alarm Query” window, from “**Alarm**” menu, click **Alarm Query**. Following figure is a typical view.



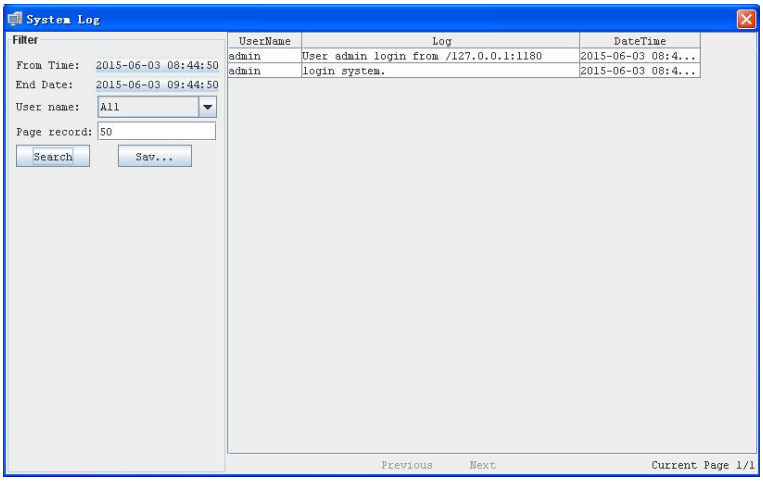
Alarm information can be queried by alarm time, alarm level, alarm status, alarm device and alarm content. The query result can be saved as a file.

On the “Alarm Log” page located on the bottom of EMS main window or open “Current Alarm” window, current alarm information can be viewed. Following figure is a typical view.



9 Operation Log Management

Operation log query feature is designed for network manager to trace back the history operation records when needed. From **Alarm** menu, click **System Log** to open operation log management window. Typical window view is shown below.



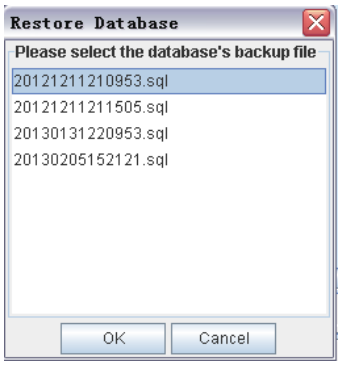
History operation log can be filter out by operation user name and operation time range. The query result can be saved as a excel file.

10 Database Maintenance

EMS database maintenance feature includes database backup and restore two functions. Most of the configuration information for EMS software, such as added device and location node, device name and user name etc. are saved in software database. To avoid configuration loss when system halted, network manager need to backup database constantly. The backup database can be restored to retrieve the original configuration when needed, such as operating system reinstalled or EMS reinstall.

Database maintenance function located on **System** menu. Click **Database Backup** in “Database Maintenance” submenu. When backup operation finished, following prompt message will appear. Software save database files using automatically generated file name. And the backup database files are saved at system default directory. Network manager can move these files to securer location if needed.

When do database restore, click **Database Restore** in “Database Maintenance” submenu. Select the database file to be restored on the pop-up window and click **OK** button to do restore operation. Typical view is shown below.

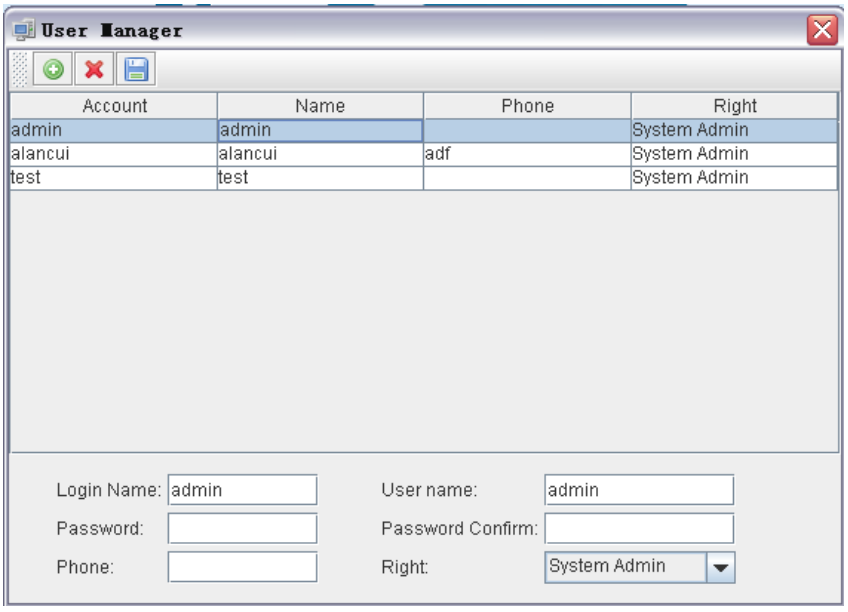


On the pop-up database restore window, only the files saved at system default directory will be list. If the backup files were moved to other location, they must be copied to the default directory first. The system default location for saving database files is "…\EMS\EMS Server\backupDB" directory.

11 User Accounts Management

EMS software supports multi-user operation, and set different privilege for different user to improve system security. Network managers can add or delete user accounts or modify their information.

Following figure is a typical operation view.



User management operations are explained as below:

Adding a User

To add a new user account, do the following:

1) Input username, password and other user account information on the text boxes located on the bottom of the user management window.
2) Choose the operation privilege level for the adding user.

3) Click **Adding User** button icon to add this new user.
4) Click **Save** button icon to save the operation results.

Deleting a User

To delete a user account, do the following:

1) Choose the user account entry list in user accounts table.
2) Click **Delete** button icon.
3) Click **Save** button icon to save the results.

Changing User Information

To change a user account configuration, do the following:

1) Choose the user account entry to be changed in user list table.
2) The chosen user information will be displayed on the bottom user account corresponding parameters.
3) Modify the displayed account information.
4) Click **Save** button icon to save the changed results.

User Account Privilege

There are "**System Admin**", "**Network Manager**" and "**Common User**" three different management privilege levels. "System Admin" level is the highest privilege, has all the operation rights of EMS software. "Network Manager" level has all the operation rights, except of user account management function. "Common User" level is the lowest privilege, the users with this privilege can only view management information and have not the rights to do any set operations.

12 System Upgrade

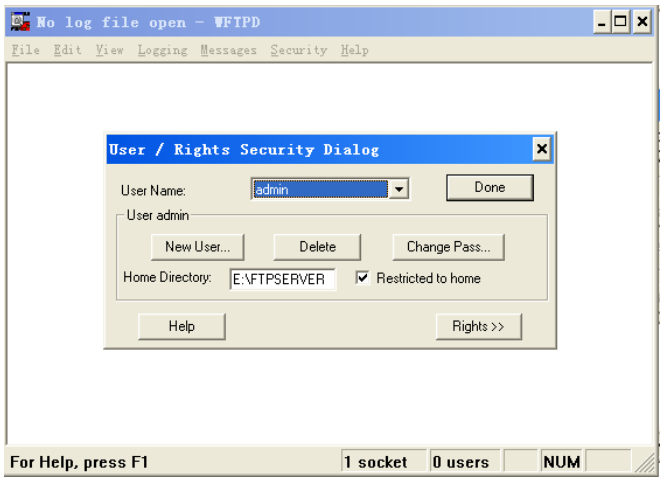
EMS software supports device firmware on-line upgrade. The main procedure for device upgrading is two steps. First, download firmware files to target devices to be upgraded. Then target device will go through the whole firmware update process according to upgrade commands received from EMS.

Device upgrading steps are introduced as follows:

1. FTP Server Configure

Install a FTP server program on the management PC if you have not. Then start the FTP server. There is a third party FTP server program "WFTPD" if EMS is fully installed. Following introduce take "WFTPD" as a sample. There may be some different if the FTP server is not WFTPD. In such condition, please refer to the software user manual.

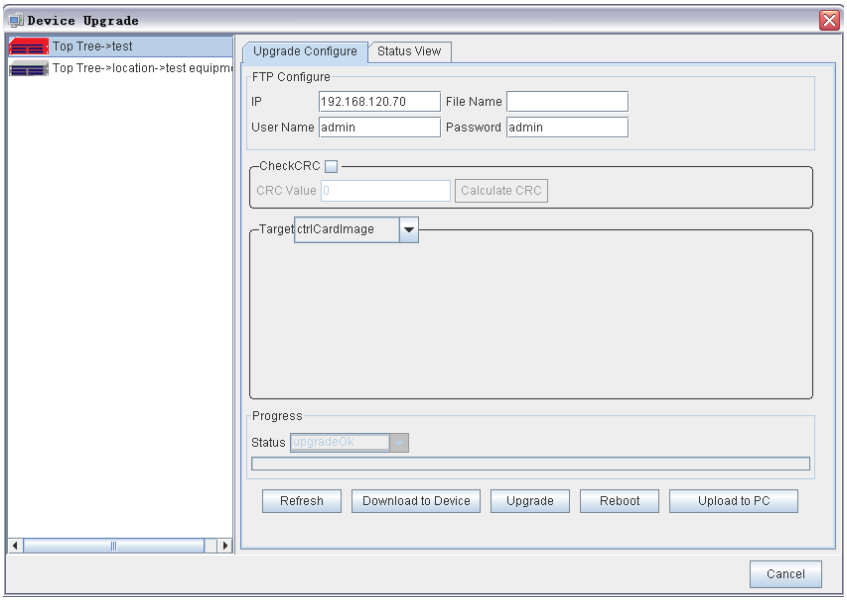
From the **Security** menu of "WFTPD" program, select **Users/rights** item to open the user security dialog window. Configure the username, access password and home directory information. Typical configuration window is shown below.



2. Copy the device firmware files to be update to the home directory of FTP server program.

3. EMS Upgrade Parameters Configuration

1） From **Configure** menu, select **Device Upgrade**. Device upgrade window will appear. Typical view is shown as below.



2） Choose the OLT device to be upgraded from the device list on the left column of window.

3） Input FTP Server IP Address, User Name, Password and Firmware file name on the “Upgrade Configure” page.

4） Select the file target to be updated.

The supported upgrade targets may be different for different type devices. For FD2000S OLT device, for example, the supported upgrade targets include switch and control card firmware, PON card firmware, PON chip firmware, PON card configuration files and PON chip boot file.

Following take WDS1U2PGE OLT device as sample to introduce upgrade procedure.

From the **Target** dropdown list to select a target file object.

5） Choose the target device object

For per target file object, some index parameters need to be chosen to specify the specific device object to be upgraded. For example, if the file target is for PON card object, then PON card slot index need to be chosen. One or more number index can be specified at the same time.

6） CRC Check

In order to avoid upgrade an error file to target devices, CRC check function can be used. Before downloading file to devices, the **Calculate CRC** tool button can be used to calculate the CRC result of the selected file. When the file is transmitted to target device, the device firmware will recalculate the CRC result and then compare this result with the CRC value received from EMS. Such feature will avoid error file is upgraded to device.

4. Upgrade Operation

When the upper needed upgrade configurations are finished, according to following steps to finish device upgrade procedure.

1） Click **Download to Device** button

In this step, the FTP client program running on device will download the target file from the specified FTP server. When finished successfully, the ‘Progress Status’ will display ‘transmit ok’ result.

2） Click **Upgrade** button

In this step, the target device will update the specified file with the new received file. When finished successfully, the **Process Status** will display “upgrade ok” result.

3） Click **Reboot** button

The new upgrade file will take effect when the target device reboot.

Whole upgrade process finished when the target device boot up with the upgraded new files.

End

Thanks for choosing the wodaplug.com products !

Contact:

Company Address：Prague. 150 00 Prague 5, Radlicka 33, Tomorrow systems s.r.o.

Tel：+420 257 21 10 10

Mail：info@wodaplug.com

Web: www.wodaplug.com